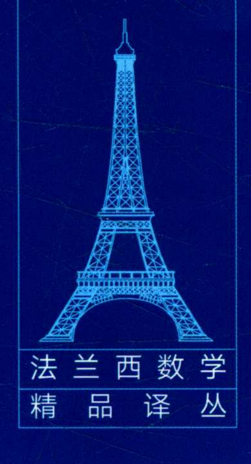


法兰西数学
精品译丛

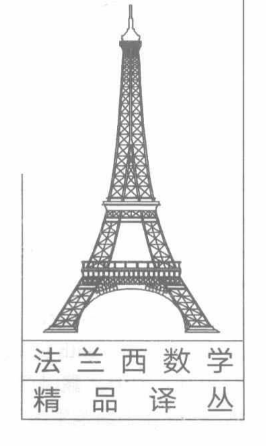
分析与代数原理（及数论）

（第二卷）（第2版）

□ Pierre Colmez 著

□ 胥鸣伟 译

高等教育出版社



分析与代数原理（及数论）

（第二卷）（第2版）

□ Pierre Colmez 著

□ 胥鸣伟 译

高等教育出版社·北京

图字：01-2018-0877 号
Éléments d'analyse et d'algèbre (et de théorie des nombres), second edition by Pierre Colmez

图书在版编目（CIP）数据

分析与代数原理（及数论）：第 2 版．第二卷 /（法）皮埃尔·科尔梅（Pierre Colmez）著；胥鸣伟译．--北京：高等教育出版社，2018. 7
ISBN 978-7-04-049869-1

Ⅰ．①分… Ⅱ．①皮… ②胥… Ⅲ．①代数②数论 Ⅳ．① O15

中国版本图书馆 CIP 数据核字（2018）第 110194 号

分析与代数原理（及数论）
FENXI YU DAISHU YUANLI (JI SHULUN)

策划编辑　吴晓丽　　责任编辑　吴晓丽　　封面设计　杨立新　　版式设计　徐艳妮
责任校对　胡美萍　　责任印制　韩　刚

出版发行　高等教育出版社
社　　址　北京市西城区德外大街4号
邮政编码　100120
印　　刷　北京汇林印务有限公司
开　　本　787 mm × 1092 mm　1/16
印　　张　28.75
字　　数　610 千字
购书热线　010-58581118
咨询电话　400-810-0598
网　　址　http://www.hep.edu.cn
　　　　　http://www.hep.com.cn
网上订购　http://www.hepmall.com.cn
　　　　　http://www.hepmall.com
　　　　　http://www.hepmall.cn
版　　次　2018 年 7 月第 1 版
印　　次　2018 年 7 月第 1 次印刷
定　　价　99.00 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换

物 料 号　49869-00

《法兰西数学精品译丛》编委会

《法兰西数学精品译丛》序

随着解析几何及微积分的发明而兴起的现代数学, 在其发展过程中, 一批卓越的法国数学家发挥了杰出的作用, 做出了奠基性的贡献. 他们像灿烂的星斗散发着耀眼的光辉, 在现代数学史上占据着不可替代的地位, 在大学教科书、各种专著及种种数学史著作中都频繁地出现着他们的英名. 在他们当中, 包括笛卡儿、费马、帕斯卡、达朗贝尔、拉格朗日、蒙日、拉普拉斯、勒让德、傅里叶、泊松、柯西、刘维尔、伽罗瓦、庞加莱、嘉当、勒贝格、韦伊、勒雷、施瓦茨及利翁斯等这些耳熟能详的名字, 也包括一些现今仍然健在并继续做出重要贡献的著名数学家. 由于他们的出色成就和深远影响, 法国的数学不仅具有深厚的根基和领先的水平, 而且具有优秀的传统和独特的风格, 一直在国际数学界享有盛誉.

我国的现代数学, 在 20 世纪初通过学习西方及日本才开始起步, 并在艰难曲折中发展与成长, 终能在 2002 年成功地在北京举办了国际数学家大会, 在一个世纪的时间中基本上跟上了西方历经四个多世纪的现代数学发展的步伐, 实现了跨越式的发展. 这一巨大的成功, 根源于好几代数学家持续不断的艰苦奋斗, 根源于我们国家综合国力不断提高所提供的有力支撑, 根源于改革开放国策所带来的强大推动, 也根源于很多国际数学界同仁的长期鼓励、支持与帮助. 在这当中, 法兰西数学精品长期以来对我国数学界所起的积极影响, 法兰西数学的深厚根基、无比活力和优秀传统对我国数学家所起的不可低估的潜移默化作用, 无疑也是一个不容忽视的因素. 足以证明这一点的是: 在我国的数学家中, 有不少就曾经留学法国, 直接受到法国数学家的栽培和法兰西数学传统和风格的熏陶与感召, 而更多的人也或多或少地通过汲取法国数学精品的营养而逐步走向了自己的成熟与辉煌.

由于语言方面的障碍, 用法文出版的优秀数学著作在我国的传播受到了较大的限制. 根据一些数学工作者的建议, 并取得了部分法国著名数学家的热情支持, 高等教育出版社决定出版《法兰西数学精品译丛》, 将法国的一些享有盛誉并有着重要作用与

影响的数学经典以及颇具特色的大学与研究生数学教材及教学参考书, 有选择地从法文原文分批翻译出版. 这一工作得到了国家自然科学基金委员会数学天元基金的支持和赞助, 对帮助并推动我国读者更好地学习和了解法国的优秀数学传统和杰出数学成就, 进一步提升我国数学（包括纯粹数学与应用数学）的教学与研究工作的水平, 将是意义重大并影响深远的, 特为之序.

李大潜

2008 年 5 月

序　言

在这本书中人们会发现一些以非常规方式反映出的法国高等教育结构的某些特性 (像大多数这类书一样, 这绝非是唯一的讨论对象). 这些特性平行地表现在传统的大学里, 在那里存在一个 "名门望校" [1] 的精英人才体系, 它极其类似于印度的种姓制 (虽然每个学校具有相对的特点, 但这个系统却被在学校之间的一个相当固定的等级划分制度所支配). 要进入名门大学必须经过竞争: 在预科班上进行两年激烈的竞争性准备.

我在巴黎综合理工大学[2] 讲授了一门课, 并由此写出这本书. 我讲课的这个学校离上述的体系还是稍稍有些距离的: 它是一所军事院校, 在那里体育运动颇多, 而且它首要的目标是培养工程师, 以充实到法国各大企业的各个岗位上. 但是它却具有科学的传统, 其中数学起了重要的作用: 蒙日、拉格朗日、泊松、拉普拉斯、傅里叶、柯西、刘维尔、埃尔米特, 还有更近代的 P. 莱维、L. 施瓦兹, 都曾是那里的教授, 同时还培养出了为数颇多的杰出数学家, 包括泊松、柯西、刘维尔、埃尔米特、庞加莱和

[1]法文是 "Grandes Écoles", 这是一个专有名词, 是指法国教育体制中独立于公共大学教育架构的高等教育机构, 是法国对通过入学考试 (concours) 来录取学生的高等院校的总称, 用来区别于大学 (université), 即持有高中会考毕业证书的学生都可以申请进入的普通高等学校. 但是只有优秀学生可以进入 "Grandes Écoles" 的预科; 经过两年的专门培养, 再经过竞争激烈的、淘汰率高的竞考, 通过者才可根据成绩双向选择, 然后进入某一所 "名门望校", 在那里学习三到四年. —— 译者注, 用方括号标出, 而书中原注用圆括号标出.

[2]法文名称是 "École Polytechnique", 有人译为巴黎综合理工学院或学校, 于 1794 年由拿破仑建立, 称得上真正的 "名门望校". 它的昵称为 "X", (见脚注 (1) 中 (X⋯) 的 X) 即表达了此意.

莱维[1].

催生了本书的这门课程力主在学生中发展数学文化 (特别关注现代数学的统一性和强大能力), 即充分展示数学在巴黎综合理工大学所教其他学科 (物理、化学、信息、经济) 中的运用. 本书可分为四个部分:

- 长长的一部数学词典, 它将预科班上见过的材料加以重组和精确化 (这不是一部教材而仅仅是一个浓缩的汇总, 并用解答习题和在书页底部给出有关的文化注解加以充实).
- 在此词典的基础上, 教程本体 (第 I 章到第 VII 章) 介绍了三个基础理论: 群表示论, 实分析 (巴拿赫空间、勒贝格积分以及傅里叶变换), 还有全纯函数论. 这里有大量习题, 有些在给出习题时已做了解答; 对于大多数习题也准备在后面给出它们正确结果的证明.
- A 到 G 七个附录开启了通向更加深刻、更为新近结果的道路, 其中在最后两个附录中所用到的完全是本教材中讲述的技术.
- 十四个习题解答 (称作习题校正): 每次应用教材中的数学对它们进行解答的同时也就是给出了对某个深刻结果的证明. 这种类型的问题似乎具有一种法国特质, 这种特质在法国数学学派的成就中多有显现. 它们对消化吸收所遇到的那些概念和结果, 对教材中所讲述的工具的威力进行评价提供了不可替代的帮助; 我的忠告则是, 在试图把握这些基本定理的证明前, 自己先去寻找解决方法 (倘若失败了, 去看一下答案; 对于根本不懂的情形, 阅读一个未曾考虑过的问题的解答无疑是个理想的方案; 反之, 尝试自己解答问题则是接受和消化这个解答的最好的准备方式); 它们也以较为初等的方式解释了数学的统一性.

---

[1]不用追溯太远, 下面是巴黎综合理工大学校友的名单 (名字后面是他们入校的年份), 他们曾受邀在国际数学家大会报告他们的工作, 这个大会每四年举行一次, 其作用在于定期地更新数学的进展 (也颁发菲尔兹奖): 1970 (尼斯), F. Pham (X1957); 1974 (温哥华), A. Bensoussan (X1960) 和 B. Maurey (X1966); 1978 (赫尔辛基), A. Raviart (X1958); 1982 (华沙), B. Mandelbrot (X1944), R. Glowinski (X1958), J.-M. Fontaine (X1962), B. Teissier (X1964) 和 G. Pisier (X1969); 1986 (伯克利), J.-M. Bismut (X1967); 1990 (东京), L. Tartar (X1965), J. Ecalle (X1966) 和 J.-M. Coron (X1975); 1994 (慕尼黑), P. Ciarlet (X1959), F. Ledrappier (X1965), A. Louveau (X1966) 和 E. Pardoux (X1967); 1998 (柏林), M. Herman (X1963), G. Iooss (X1964), A. Lascoux (X1964), J.-M. Bismut (X1967), G. Pisier (X1969), S. Mallat (X1981), F. Hélein (X1983) 和 F. Béthuel (X1983); 2002 (北京), J.-M. Fontaine (X1962), A. Chenciner (X1963), P. Flajolet (X1968), P. Delorme (X1970), A. Cohen (X1984) 和 T. Rivière (X1987); 2006 (马德里), F. Morel (X1984), C. Lebris (X1986) 和 E. Candès (X1990); 2010 (海得拉巴), J.-M. Coron (X1975), F. Pacard (X1984) 和 C. Breuil (X1989). 但这远不能与巴黎高等师范学院及其十位菲尔兹奖得主 (施瓦兹 (L. Schwartz)、塞尔 (J.-P. Serre)、托姆 (R. Thom)、孔涅 (A. Connes)、利翁斯 (P.-L. Lions)、约科茨 (J.-C. Yoccoz)、拉弗格 (L. Lafforgue)、维尔纳 (W. Werner)、维拉尼 (C. Villani) 和吴宝珠 (Ngô Bao Châu)) 相比肩, 然而作为一所工科加军事的院校, 这已是非常卓越了 (巴黎高等师范学院的作用是培养高水平的学者).

在写这本书的过程中我也学到了许多, 也希望读者在这里能找到满足他们好奇心的东西. 作为一位数论学家, 我为能从数论中给出解释数学统一性[2] 问题颇感荣耀; 但愿有与物理学关系密切的人能够写出由物理学启迪的附录, 以及它所涉及的数学术语和第 I 到第 VII 章的数学.

Pierre Colmez

[2] 观察一些概念如何与一个理论相互印证或者从一个领域过渡到另一个是十分迷人的; 小词典的注 47 给出了一个相当令人吃惊的解释. 同样地, 问题 H.9 也受到 p-adic 理论的定理 D.3.2 的启发, 对此我曾自问, 它在实域 (或复域) 中会变成什么样? 后来我才意识到, 按照 Paley-Wiener 定理的思路看来, 它完全是一个经典的结果.

前　　言

数学是一个具有惊人威力的工具, 其他的科学分支都以不同的方式在不同程度应用它, 同时它又是人类最不可思议的集体造物中的一个, 并且人类一代接一代地使得这座大厦不断地升高但仍矗立在坚实的基础之上. [1]

本书介绍了作为数学基石的理论中的三个. 第一个 (第 I 章) 是有限群的表示论及其特征标; 这个理论是在 1895 到 1905 年间由弗罗贝尼乌斯 (F. Frobenius)、伯恩赛德 (W. Burnside) 和舒尔 (I. Schur) 发展起来的, 它是线性代数的一个推广 (涉及对由多个同构生成的群在一个有限维向量空间上的共同作用的理解), 而特征标理论则是在有限架构上的傅里叶变换的一个最重要的表现方式, 在此架构上没有分析上的难点. 在数学中, 在一些物理分支 (譬如粒子物理) 中, 或者还在经典化学的一个小方向 (晶体) 上, 群表示论处于中心的位置; 有限群的情形也常常被作为在更加复杂情形中进行合理推测的一个先导.

第二个 (第 II, III, IV 章) 是在 1900 到 1930 年发展起来的泛函分析 (巴拿赫空间、勒贝格积分、傅里叶变换), 为此做出贡献的有贝尔 (R. Baire)、巴拿赫 (S. Banach)、弗雷歇 (M. Fréchet)、哈恩 (H. Hahn)、希尔伯特 (D. Hilbert)、勒贝格 (H. Lebesgue)、普朗谢雷尔 (M. Plancherel)、里斯 (F. Riesz)、施坦豪斯 (H. Steinhaus), …… 这个理论因 20 世纪对微分方程和偏微分方程等锲而不舍的追求而诞生, 它形成了现代实分析的基础. 在由物理提出的偏微分方程 (热传导方程、波动方程、薛定谔方程, ……) 的研究中, 它有着多不胜数的应用.

最后一个 (第 V, VI, VII 章) 介绍了单复变量的解析函数理论, 它是在 1820 到 1840 年间由柯西一手发展起来的, 后来他还定期地返回这个领域; 本书所依照的讲述方式大多应归于魏尔斯特拉斯和庞加莱在 19 世纪后半叶所做的贡献. 这个理论, 还有群的一般理论, 大概是在别的数学分支或理论物理中用的最多的两个了. 例如, 平面开集的共形表示在具平面区域边界条件的热传导方程、空气动力学、布朗运动或者聚合 [2]

物等的研究中都有应用, 我们将只简短提及它们 (第 VI 章的注 1).

这类教材的一个主要问题在于, 虽然它们着重关注那些将来有很大应用的结果, 但却将这些应用只是作为趣味数学归入到习题之中, 这就好像人们只是为了对教堂立柱基座的经年的坚固性感兴趣而去参观它那样. 为了努力改变这种倾向, 我们将注意力集中在来自数论方面的分析课题上; 数论具有与几乎所有数学领域 (甚至理论物理) 相互作用的惊人能力, 从而对这些领域的进展做出强有力的贡献. 它涉及 L 函数, 它的原型是黎曼 ζ 函数 (定义为: 当 $\mathrm{Re}(s)>1$ 时, $\zeta(s)=\sum_{n=1}^{+\infty}\frac{1}{n^s}$). 有关这些对象的主要结果之一大概要数欧拉 (1734) 的著名公式 $\zeta(2)=\frac{\pi^2}{6}$ 了, 它回答了在 1644 年提出的知名的 "巴塞尔 (Bâle) 问题". 同样是欧拉, 揭示了 ζ 函数与素数分布之间的关联, 但它一直没有被严格证明. 直到 1896 年, 阿达马 (J. Hadamard) 和德拉瓦莱普森 (C. de la Vallée Poussin) 才按照黎曼在 1858 年提出的方案给出了正确的证明. 其间, 狄利克雷 (G. Dirichlet) 在 1837 年引进了第一批 L 函数, 用来证明在算术级数中存在无穷多个素数. 附录 A 专门讨论了这些结果, 它还提供了对全纯函数用处的令人震惊的诠释: 在那里它被用来解决看起来非常难的问题. 自此之后, L 函数的范围得到了充实, 形成了一个壮观的大厦, 为此, 附录 G 力图从观察给出一些见解, 就像去巴黎圣母院应鉴赏其穹窿的优美和雄伟, 而没有必要弄懂为什么它没有垮塌, 更没有必要去了解如何进行建造才不会引起逐步坍塌. 我们自己则只限于 L 函数的解析性方面, 它涉及另一个无所不在且十分令人激动的数学对象, 即模形式; 按照前面所说的方案我们将它归并成一系列的习题. 我们 (差不多) 抵制住了想要探索 L 函数的算术性质的诱惑: 它们在整数上的取值隐藏着一些宝藏, 包括德利涅 (P. Deligne) 的总猜想中的一些对象 (该猜想 (1977) 合理地给出了关于 π^2 的欧拉公式, 以及不可能存在 $\zeta(3)$ 的 π^3 公式), 贝林森 (A. Beilinson) 的猜想 (1985, 他特别要寻求在 $\zeta(3)$ 中究竟包含了什么东西的某种解释), 还有布洛赫 (S. Bloch) 和加藤 (K. Kato) 的猜想 (1989, 他们的猜想是要给出一个完全一般的公式, 譬如, 它能告诉我们在公式 $\zeta(12)=\frac{691\pi^{12}}{3^6\cdot5^3\cdot7^2\cdot11\cdot13}$ 中的 691 有什么意义). 伯奇 (Birch) 与斯温纳顿–戴尔 (Swinnerton-Dyer) 猜想是这些隐匿的宝藏的一个例子; 这个猜想是在 20 世纪 60 年代初提出的, 附录 F 将专门讨论它. [3]

参考文献概览

希望更加深入了解本书某些课题的读者请参看下面所列的著作[1]. 这些著作与本书的水平几乎相当, 但要更关注某些特定的方向, 它们能让读者走得更远.

P. Biane, J-B. Bost 和 P. Colmez, *La fonction zêta*, Presses de l'École Polytechnique.

读者在这里可发现 ζ 函数与算术或概率论相关联的各个不同方面.

---

[1] 构造习题的标准办法是, 拿出在比较专门的著作中的结果然后加以剪辑形成问题. 因此读者可以在这些著作中找到本书大部分习题的答案.

J-B. Bost, *Fonctions analytiques d'une variable complexe*, École Polytechnique.

覆盖了本书的 V 到 VII 章和附录 A 的一部分.

D. Bump, *Automorphic forms and representations*, Cambridge University Press.

附录 G 的展开版本; 读这本书要求有大量的时间和精力的投入.

H. Cartan, *Théorie élémentaire des fonctions analytique d'une ou plusieurs variables complexes*, Hermann.

覆盖了 V 到 VI 章, 但追循的是几何方向 (黎曼面以及多变量函数).

W. Ellison, *Les nombres premiers*, Hermann.

除覆盖了附录 A 外还有更多的内容.

W. Fulton 和 J. Harris, *Representation theory, A first course*, GTM 129, Springer-Verlag.

由第 I 章和附录 C 开始, 但追循的是李群表示论的方向.

R. Godement, *Analyse mathématique II,III et IV*, Springer-Verlag.

覆盖了本教材的最重要部分, 我曾希望, 如果能得到允许, 直接在本书中加入该书中的数页内容. 该书对于模形式的处理相当到位.

N. Koblitz, *Introduction to elliptic curves and modular forms*, GTM 97, Springer-Verlag.

提供了对数论的一个概览, 可关联到同余数问题 (附录 F).

S. Patterson, *An introduction to the theory of the Riemann Zeta-functions*, Cambridge University Press.

覆盖了附录 A, 追寻的是黎曼和林德勒夫假定.

W. Rudin, *Real and Complex Analysis*, Mc Graw-Hill.

分析教材, 特别地覆盖了分析部分 (II 到 VI 章), 但它并没有停留在此而是走得更远.

J-P. Serre, *Cours d'arithmétique*, Presses Universitaires de France. [4]

一本深入学习有理系数二次形式和模形式的令人愉悦的书.

J-P. Serre, *Représentations Linéaires des groupes finis*, Hermann.

覆盖了第 I 章和附录 C 的一部分, 并继续讨论涉及有限群表示论的更深刻的问题.

A. Weil, *Elliptic functions according to Eisenstein and Kronecker*, Springer-Verlag.

一本读起来舒服的带有半历史性的书, 用初等语言讲解了全纯函数与数论之间的关联.

最后, 有两本关于数学思想史的书, 本书的脚注很多来自它们. 这两本书所覆盖的

时间段尽管是非空交集但不完全相同; 第二本要更近代一些, 要求有更扎实一点的数学背景.

A. Dahan-Dalmedico 和 J. Peiffer, *Une histoire des mathématiques, routes et dédales*, Points Sciences, Éditions du Seuil.

J. Dieudonné, *Abrégé d'histoire des mathématiques*, Hermann.

[5] 标准符号

以 $\mathbf{N}$ 表示自然数集 $\{0,1,2,\ldots\}$, $\mathbf{Z}$ 为整数集, $\mathbf{Q}$ 为有理数域, $\mathbf{R}$ 为实数域而 $\mathbf{C}$ 为复数域. 以 $\mathbf{Q}^*$, $\mathbf{R}^*$, $\mathbf{C}^*$ 分别表示 $\mathbf{Q},\mathbf{R},\mathbf{C}$ 的乘法群.

$\mathbf{R}_+$ (分别地, $\mathbf{R}_+^*$) 表示正实数集 (分别地, 严格正实数集); 而 $\mathbf{R}_-$(分别地, $\mathbf{R}_-^*$) 表示负实数集 (分别地, 严格负实数集).

以 $\overline{\mathbf{R}}=\mathbf{R}\cup\{\pm\infty\}$ 表示扩张实直线, $\overline{\mathbf{R}}_+=\mathbf{R}_+\cup\{+\infty\}$ 表示扩张的实半直线.

如果 $t\in\mathbf{R}$, 以 $[t]$ 表示它的整数部分, 而 $\{t\}=t-[t]$ 表示它的分数部分.

如果 X 是个集合, 以 $|X|\in\mathbf{N}\cup\{+\infty\}$ 表示它的基数; 如果 $Y\subset X$, 则以 $\mathbf{1}_Y:X\to\{0,1\}$ 表示 Y 的特征函数 (定义为: 当 $x\in Y$ 时, $\mathbf{1}_Y(x)=1$, 而当 $x\notin Y$ 时, $\mathbf{1}_Y(x)=0$). 如果 X,Y 为集合 E 的两个子集, 记 $X-(X\cap Y)$, 或更简单地, $X-Y$ 为 $X\cap Y$ 在 X 中的补集.

如果 I 和 X 均为集合, 以 X^I 表示 I 到 X 的映射的集合; 记 X^I 中的一个元素为 $i\mapsto x_i$ 或 $i\mapsto x(i)$, 再或者 $(x_i)_{i\in I}$ (例如当 $I=\mathbf{N}$ 时).

我们常常以 "$a,b\in X$" 记 "$a\in X$ 和 $b\in X$", 而且我们对于所有的量化词均不加解释: 例如, 我们常以 "当 $|x|\leqslant\delta$ 时, $|f(x)|\leqslant\varepsilon$" 代替 "对所有的 $|x|\leqslant\delta$, $|f(x)|\leqslant\varepsilon$".

设 A 是个环, $n\in\mathbf{N}-\{0\}$. 我们以 $\mathbf{M}_n(A)$ 表示系数在 A 中的 $n\times n$ 矩阵组成的环, $\mathbf{GL}_n(A)\subset\mathbf{M}_n(A)$ 为可逆矩阵的群 (它的行列式在 A 中可逆), 而 $\mathbf{SL}_n(A)$ 是 $\mathbf{GL}_n(A)$ 中行列式为 1 的矩阵的子群.

$x\gg 0$ (分别地, $x\ll 0$) 代表充分大 (分别地, 充分小) 的实数.

如果 f,g 是从拓扑空间 X 到 $\mathbf{R}$ 或 $\mathbf{C}$ 的函数, 在 x_0 的邻域中记号 $f=O(g)$ 的意思是, 存在 x_0 的一个邻域 V 和一个常数 $C>0$, 使得对 $x\in V$ 有 $|f(x)|\leqslant C|g(x)|$; 在 x_0 的邻域中记号 $f=o(g)$ 表示存在 x_0 的一个邻域 V 及一个在 x_0 处趋于 0 的函数 $\varepsilon:V\to\mathbf{R}_+$, 使得对所有 $x\in V$, 有 $|f(x)|\leqslant\varepsilon(x)|g(x)|$.

目　　录

第一卷的内容

数学小词典

I. 有限群的表示

[231]

如果 G 是一个群, G 的一个表示 V 是一个在域 K 上的向量空间 V(或者, 更一般地, 在一个环 A 上的模) 连同其上的一个 G 的线性作用 (即对每个 $g \in G$, 要求 $x \mapsto g \cdot x$ 是 V 到 V 的一个线性映射). G 和 V 常常被赋予了拓扑, 于是, 一般地要求 $(g, x) \mapsto g \cdot x$ 是从 $G \times V$ 到 V 的连续映射.

群表示以多种方式出现在数学、物理或者化学之中. 例如, 有限群的表示论的最初动机之一便来自晶体学. 粒子物理极大地利用了如群 $\mathbf{SU}(2)$ 这样的李群的表示, 这时 $\mathbf{C}^2$ 中的行列式为 1 的等距变换群 (具有通常的标量积 $\langle (x_1, x_2), (y_1, y_2) \rangle = \overline{x_1} y_1 + \overline{x_2} y_2$), 或者系数为实的上幂幺的 3×3 矩阵 (即对角为 1 的上三角矩阵) 的海森伯群, 或者还有洛仑兹 (即 $\mathbf{O}(1,3)$) 和庞加莱群.

如果 G 是一个群, 关于 G 的表示的知识则提供了许多关于 G 本身的信息, 而且某些群也只有通过它们的表示才能被了解. 举例来说, 基数为

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

的最大散在单群大魔群的存在性问题[1] 为格里斯 (R. Griese) 在 1982 年所证明. 这 [232]

---

[1]一个群 G 为单是说它的仅有的正规子群只有 $\{1\}$ 和 G 自己. 如果一个有限群不是单的, 它则具有一个非平凡的正规子群 H, 而 H 和 G/H 是两个比 G 更小的群, 于是可由它们去构造 G. 迭代此过程将任意的有限群分裂出一个单群的有限族. 有限群的分类于是化成为有限单群的分类, 从而可以了解如何将这些单群组合起来做成更大的群. 有限单群的分类在 20 世纪 80 年代初期取得成功 (它写满了成千页, 人们确实掌握全部的 ……). 这个分类由一些无限族组成, 诸如对于所有素数 p 的 $\mathbf{Z}/p\mathbf{Z}$, 另外还有对 $n \geqslant 5$ 时的交错群 A_n, 和对其中心取商的 $\mathbf{SL}_n(\mathbf{F}_q)$ (其中 $\mathbf{F}_q$ 是具 q 个元的域), 以及其他一些由谢瓦莱 (C.Chevalley) 在 1954 年发现的群, 而除去这些族外, 还有 28 个孤立的群, 譬如散在群.

是由于他构造了它们的表示中的一个 (具 196883 维) 才取得了成功[2], 于是才有了在 1973 年被格里斯和菲舍尔 (B. Fischer) 预测过的大魔群的存在性 (这有点像对于基本粒子的追索).

同样地, 考虑在代数数域 $\overline{\mathbf{Q}}$ 上的自同构群 $\mathscr{G}_{\mathbf{Q}}$(参看附录 G) 的表示. 它给出了 $\overline{\mathbf{Q}}$ 上一些准确的信息, 从而能够解决数论中的一些经典问题. 例如, 怀尔斯 (A. Wiles) 对费马大定理的证明 (1994) 是把 $\mathscr{G}_{\mathbf{Q}}$ 的两种类型的表示联系起来以便引出矛盾: 一方面是来自方程 $y^2 = x(x-a^p)(x+b^p)$ 的解 (在 $\overline{\mathbf{Q}}$ 上) 的表示, 其中 $a^p + b^p = c^p$ 是费马大定理的一个可能的反例, 而另一方面则是来自模形式的那些表示.

$\mathscr{G}_{\mathbf{Q}}$ 作用在 $\overline{\mathbf{Q}}$ 上的例子事实上是相当典型的, 如果有一个群 G 作用在一个集合 X 上, 并且如果我们已经清楚了解了 G 的表示, 那么就可以期待得出 X 上的详细信息. 这个对称性原理在现代的理论物理中起着不可忽视的重大作用.

表示论呈现出两个方面的特征. 第一个方面 (表示的不可约表示分解) 是自同态约化 (特征值、特征空间、对角化) 的推广, 经过一些小小的转换 (习题 I.1.2 和 I.2.3, 注记 I.2.4), 它对应于群 $\mathbf{Z}$ 的情形. 第二个方面 (特征标理论) 则是在非交换 (或交换, 参考 I.2 小节的 5.1 节) 框架下的傅里叶分析的第一阶近似. 除了可以与经典的线性代数联系的情形 $\mathbf{Z}$ 外, 我们在本教程中本质上只考虑有限群的复表示. 这种情形的好处不但在于它是简单的 (不需要纠缠于收敛性问题或者其他一些可能遇到的分析中的微妙差异, 譬如, 在对应于群 $\mathbf{R}/\mathbf{Z}$ 的傅里叶级数的研讨中), 而且在别的场合成立的某类陈述有希望在这里也有完全的类似断言. [233]

I.1. 表示与特征标

1. 群的表示, 例题

读者可以参阅数学小词典的 2.11.1 小节, §3 和 10.1 小节的线性代数和群论的基础知识的术语和结论.

设 G 为群, 群运算 $(g,h) \mapsto gh$, G 的一个*表示* V 是一个 $\mathbf{C}$-向量空间, 其上有 G 的一个线性的 (左) 作用. 这样一个表示等价于 G 的一个到 $\mathrm{GL}(V)$ 的群态

[2]这是大魔群的最小的一个非平凡表示; 大魔群的不可约表示的维数列表中的最初几个是

$$f_1 = 1,\ f_2 = 196883,\ f_3 = 21296876,\ f_4 = 842609326,\ f_5 = 18538750076,\ f_6 = 193600625727, \ldots$$

J. Mckay 在 1977 年注意到, 196883 与模函数 j (参看习题 VII.6.10) 的傅里叶级数的系数有关: 如果将 $j(z)$ 写成形式 $j(z) = \frac{1}{q} + 744 + \sum_{n\geqslant 1} c_n q^n$, 其中 $q = e^{2i\pi z}$, 于是 $c_1 = f_2 + f_1$, $c_2 = f_3 + f_2 + f_1$, $c_3 = f_4 + f_3 + 2f_2 + 2f_1, \ldots$. 看看所列出来的这些庞大的数, 出现这样的偶然巧合的机会应该是很少的. 以 "大魔群的梦话 (monster's moonlight)" 而为人所知的这个巧合的秘密被 R. Borcherds 在 1992 年利用来自数学物理的一些对象所揭晓, 为此他获得了菲尔兹奖 (1998). "monster's moonshine" 不像字面上表达的那样具有诗意, 因为 "moonshine" 应该取 "愚蠢, 胡说" 的含义, 就像 E.Rutherford 的下面的引语所表达的:"原子破裂所释放的能量是一件微不足道的事. 任何人期望从原子的这些转化得到能源是在说胡话 (talking moonshine)."

射 ρ_V: 如果 $g \in G$, 映射 $v \mapsto g \cdot v$ 是一个线性的双射, 从而定义了 $\mathrm{GL}(V)$ 中的一个元 $\rho_V(g)$, 而对于任意的 $g, h \in G$ 和 $v \in V$ 有恒等式 $g \cdot (h \cdot v) = gh \cdot v$, 它也可化为恒等式 $\rho_V(gh) = \rho_V(g)\rho_V(h)$. 后面我们将不加区别地谈及 G 的表示 V 或者 G 的表示 ρ_V, 这在于要看我们是着重于表示的向量空间还是 G 到 $\mathrm{GL}(V)$ 的态射. 有时我们也以 $\rho_{V,g}$ 记 $\mathrm{GL}(V)$ 的元 $\rho_V(g)$, 从而可以以 $\rho_{V,g}(v)$ 代替 $\rho_V(g)(v)$ 这个 $v \in V$ 在 $g \in G$ 作用下的像 $g \cdot v$.

注记 I.1.1. — (i) 表示的平凡例子是 $\mathrm{GL}(V)$ 的子群 G 在 V 上的作用. 譬如, 正交换 $\mathbf{O}(d)$ 在 $\mathbf{GL}_d(\mathbf{R})$ 中的包含映射将 $\mathbf{R}^d$ 做成了 $\mathbf{O}(d)$ 的一个表示.

(ii) 如果 ρ_V 为单射, 则说 V 是 G 的一个忠实表示, 这时 ρ_V 让抽象的群 G 以具体的方式 (用作术语) 表示为 $\mathrm{GL}(V)$ 的一个子群. 如果 V 为有限维空间, 基的选取给出了一个作为矩阵群的更加具体的表示.

例题 I.1.2. — ($\mathbf{Z}$ 的表示)

(i) 如果 $\lambda \in \mathbf{C}^*$, 则 $n \mapsto \lambda^n$ 是从 $\mathbf{Z}$ 到 $\mathbf{C}^*$ 中的群态射, 我们将其做成一个 $\mathbf{Z}$ 的表示, 记为 $\mathbf{C}(\lambda)$; $n \in \mathbf{Z}$ 在 $v \in \mathbf{C}$ 上的作用有 $\rho_{\mathbf{C}(\lambda),n}(z) = \lambda^n z$(也可将其写为形式 $n \cdot z = \lambda^n z$).

(ii) 如果 V 是一个 $\mathbf{C}$-向量空间, 又若 $u : V \to V$ 是个线性同构, 而映射 $n \mapsto u^n$ 是从 $\mathbf{Z}$ 到 $\mathrm{GL}(V)$ 的群态射, 于是将 V 做成了加群 $\mathbf{Z}$ 的一个表示, 其中 $n \in \mathbf{Z}$ 在 $v \in V$ 上的作用由 $n \cdot v = u^n(v)$ 给出. 反之, 如果 V 是 $\mathbf{Z}$ 的一个表示, 若令 $u = \rho_V(1) \in \mathrm{GL}(V)$, 则 $\rho_V(n) = u^n$, $n \in \mathbf{Z}$, 故对于 $n \in \mathbf{Z}$ 和 $v \in V$ 有 $n \cdot v = u^n(v)$. 换句话说, $\mathbf{Z}$ 的一个表示不外乎是给出的一个 $\mathbf{C}$-向量空间 V 和一个 $\mathrm{GL}(V)$ 中的元 u.

例题 I.1.3. — ($\mathbf{Z}/D\mathbf{Z}$ 的表示) 如果 V 是一个 $\mathbf{C}$-向量空间, 且其上有一个满足 $u^D = 1$ 的线性同构 u, 则映射 $n \mapsto u^n$ 是一个从 $\mathbf{Z}$ 到 $\mathrm{GL}(V)$ 的群态射, 其核包含了 $D\mathbf{Z}$; 因而诱导了从 $\mathbf{Z}/D\mathbf{Z}$ 到 $\mathrm{GL}(V)$ 的一个态射, 它将 V 做成了 $\mathbf{Z}/D\mathbf{Z}$ [234] 的一个表示, 其上 $n \in \mathbf{Z}$ 在 $v \in V$ 的作用由 $n \cdot v = u^n(v)$ 给出. 反之, 如果 V 是 $\mathbf{Z}/D\mathbf{Z}$ 的一个表示, 且如果 $u = \rho_V(1) \in \mathrm{GL}(V)$, 则因为在 $\mathbf{Z}/D\mathbf{Z}$ 中 $D = 0$, 故 $u^D = \rho_V(D) = \rho(0) = 1$. 换句话说, $\mathbf{Z}/D\mathbf{Z}$ 的一个表示不外乎是给出一个 $\mathbf{C}$-向量空间以及 $\mathrm{GL}(V)$ 中的一个满足 $u^D = 1$ 的元 u.

注记 I.1.4. — 在上面的两种情形中, 我们从生成元 (在第二种情形, G 由 1 生成) 和这些生成元间的关系出发 (在 $\mathbf{Z}$ 的情形不存在关系, 而 $\mathbf{Z}/D\mathbf{Z}$ 有一个关系 $D = 0$), 给出了一个群的表示. 这让我们描述 G 的一个表示可以说成是在每个生成元和生成元之间的关系上赋予它们在 G 的作用下的它们之间的关系. 这种描述在处理群 G 的相对简单的表示时是非常有效的.

举例来说, 群 $\mathbf{Z}^2$ 由 $e_1 = (1,0)$ 和 $e_2 = (0,1)$ 生成, 并由交换关系 $e_1 + e_2 = e_2 + e_1$ 描述. 于是 $\mathbf{Z}^2$ 的一个表示是给出的一个 $\mathbf{C}$-向量空间 V 和 $\mathrm{GL}(V)$ 中可相互交换的两个元.

群 $\mathbf{SL}_2(\mathbf{Z})$ 由矩阵 $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ 和 $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 生成, S 与 T 之间的全部关系是关系 $S^4 = \mathbf{1}$, $S^2T = TS^2$ 和 $(ST)^3 = S^2$ 的推演结果. 故群 $\mathbf{SL}_2(\mathbf{Z})$ 的表示是给出的一个 C-向量空间 V 和 $\mathrm{GL}(V)$ 的两个元 u 和 v, 它们满足 $u^4 = 1$, $u^2v = vu^2$ 和 $(uv)^3 = u^2$.

同样, 下面的习题证明 $\{1,2,3\}$ 的置换群 S_3 的表示恰好是一个 $\mathbf{C}$-向量空间 V 以及它的两个对称元 s_1 和 s_2, 它们满足 $s_1s_2s_1 = s_2s_1s_2$.

习题 I.1.5. — 设 $\sigma_1, \sigma_2 \in S_3$ 为置换 $(1,2)$ 和 $(2,3)$.

(i) 验证 $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ 是置换 $(1,3)$.

(ii) 证明 σ_1, σ_2 生成 S_3.

(iii) 证明 σ_1 和 σ_3 之间的所有关系都是 $\sigma_1^2 = \sigma_2^2 = 1$ 和 $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ 的推论. (我们将证明一个长 $n \geqslant 4$ 的关系总可以化为一个长为 $n-2$ 的关系.)

V 的维数 $\dim V$ 就是指 $\mathbf{C}$-向量空间 V 的维数. 例如, 对所有的 $\lambda \in \mathbf{C}^*$, $\dim C(\lambda) = 1$.

自此之后, 所有的表示都暗含着是有限维的假设. 如果 $\dim V = d$, 且 $(e_1, \ldots, e_d)$ 为 V 的一组基, 则以 $R_V(g)$ 或者 $R_{V,g}$ 表示 $\rho_V(g)$ 在基 $(e_1, \ldots, e_d)$ 下的矩阵 (它依赖基的选取尽管它没有出现在记号之中). 因此 $R_V : G \to \mathbf{GL}_d(\mathbf{C})$ 是一个群态射.

习题 I.1.6. — (构造 S_3 的一个 2 维表示)

设 $A = (1,0), B = (-\frac{1}{2}, \frac{\sqrt{3}}{2})$ 以及 $C = (-\frac{1}{2}, -\frac{\sqrt{3}}{2})$. 点 A, B, C 是一个等边三角形的顶点, 三角形的重心为 $O = (0,0)$. 平面的等距变换使此三角形稳定而使 O 不动, [235] 从而是线性的; 于是它们构成了 $\mathbf{O}(2) \subset \mathbf{GL}_2(\mathbf{C})$ 的一个子群[(3)] D_3. D_3 到 $\mathbf{GL}_2(\mathbf{C})$ 的单射使得 $\mathbf{C}^2$ 成为群 D_3 的一个表示; 我们将证明这个群同构于 S_3, 这便构造出我们的 S_3 的一个表示. D_3 的一个元使集合 $\{A, B, C\}$ 稳定从而给出了从 D_3 到 $\{A, B, C\}$ 的置换群 $S_{\{A,B,C\}}$ 的一个群态射 f. 因为 A, B, C 不共线, 故 D_3 的一个元被 A, B, C 的像唯一决定, 这意味着 f 是单的. 另外, 因为 D_3 包含相对于直线 $(OA), (OB)$ 和 (OC) 的对称变换, 它分别为对换 $(B, C), (A, C)$ 和 (A, B), 而在以角 $0, \frac{2\pi}{3}$ 和 $\frac{-2\pi}{3}$ 的旋转下的像分别为循环 (A, B, C) 和 (A, C, B). 总起来, $f : D_3 \to S_{\{A,B,C\}}$ 是一个群同构, 从 $\{1,2,3\}$ 到 $\{A, B, C\}$ 的双射 $1 \mapsto A$, $2 \mapsto B$ 和 $3 \mapsto C$ 则给出了一个同构 $g : S_3 \cong S_{\{A,B,C\}}$. 将 $f^{-1} \circ g : S_3 \to D_3$ 与 D_3 到 $\mathbf{GL}_2(\mathbf{C})$ 的单射复合便得到了 S_3 到 $\mathbf{GL}_2(\mathbf{C})$ 的一个群态射. 这个映射把 $\mathbf{C}^2$ 做成了 S_3 的一个表示.

注记 I.1.7. — 设 G 是一个有限群; G 的每个元从而具有限阶. 设 V 是 G 的一个表示. 如果 $g \in G$ 的阶为 n, 则有 $\rho_V(g)^n = \rho_V(g^n) = 1$. 由于多项式 $X^n - 1$ 的根均为单根, 这表明 $\rho_V(g)$ 可对角化, 并由于 $\rho_V(g)$ 的特征值是 $X^n - 1$ 的根, 故它们是单

[(3)] 更一般地, 以 D_n 代表一个正 n 边形不变的平面等距变换群.

位根.

习题 I.1.8. — (i) 设 $V = \mathbf{C}^2$ 是在例题 I.1.6 构造的 S_3 的表示. 证明不存在 V 的基, 使 S_3 的每个元在其上的作用矩阵可同时为对角的.

(ii) 设 V 为 $\mathbf{C}$ 上的有限维向量空间, 而 u_1, u_2 是两个相互交换的可对角化的自同态. 证明 u_1 的每个特征空间在 u_2 下稳定. 由此推出存在 V 的一组基, 使得在其上的 u_1 和 u_2 的两个矩阵全是对角的.

(iii) 设 G 是有限的交换群, 而 V 是 G 的一个表示. 证明存在 V 的一组基使得在其上, 对 $g \in G$ 的矩阵 $R_V(g)$ 都是对角的. 由此推出 V 可分解为在 G 下不变的直线的直和.

2. 表示的特征标, 例题

V 的特征标 χ_V 是一个从 G 到 $\mathbf{C}$ 的一个由 $\chi_V(g) = \mathrm{Tr}(\rho_V(g))$ 定义的映射, 其中 $\mathrm{Tr}(\rho_V(g))$ 代表自同态 $\rho_V(g)$ 的迹; 它也是在 V 的任何一组基下的矩阵 $R_V(g)$ 的迹, 它还是 $\rho_V(g)$ 的计重数的特征值的和.

我们特别有 $\chi_V(1) = \mathrm{Tr}(1) = \dim V$; χ_V 在中性元的值因而是个整数; 称这个整数为特征标 χ_V 的次; 按前面所述它也是表示 V 的维数; 这一点会不断地被用到. 另外, 如果 A, B 是 $\mathbf{M}_d(\mathbf{C})$ 中的两个元, 由于 $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, 则有

$$\mathrm{Tr}(\rho_V(hgh^{-1})) = \mathrm{Tr}(\rho_V(h)\rho_V(g)\rho_V(h)^{-1}) = \mathrm{Tr}(\rho_V(g)),$$

这表明 χ_V 是 G 上的中心函数 (即 χ_V 在 G 的每个共轭类的每个元上取常值: 对任意的 $h, g \in G$ 有 $\chi_V(hgh^{-1}) = \chi_V(g)$).

注记 I.1.9. — 如果 G 有限, 而 $g \in G$, 则 $\rho_V(g)$ 的特征值为单位根. 特别地, 它们的模为 1, 从而如果 λ 是 $\rho_V(g)$ 的一个特征值, 则 $\lambda^{-1} = \bar{\lambda}$. 由于 $\rho_V(g^{-1}) = \rho_V(g)^{-1}$ 是 $\rho_V(g)$ 的逆, 并且由于迹为特征值的和, 故由此得到: 对任意的 $g \in G$ 有 $\chi_V(g^{-1}) = \overline{\chi_V(g)}$. [236]

2.1. 线性特征标

如果 V 的维数为 1, V 的自同态是个位似变换, 而带有这个位似比率的映射诱导了 $\mathrm{GL}(V)$ 到 $\mathbf{C}^*$ 的一个同构. 一个一维的表示因此是群态射 $\chi : G \to \mathbf{C}^*$; 常常称这样的态射为 G 的线性特征标. 以 $\widehat{G}$ 记这些线性特征标的集合.

如果 V 是个对应于线性特征标 χ 的 1 维表示, 则以显然的方式有 $\chi_V = \chi$. 换而言之, 一个线性特征标的特征标就是这个线性特征标自己.

记为 $\mathbf{1}$ 的平凡表示是对应于平凡特征标 $\chi : G \to \mathbf{C}^*$, 对所有 $g \in G$ 满足 $\chi(g) = 1$ 的 1 维表示.

如果 V 是 G 的一个表示, 而 $\chi \in \widehat{G}$, 我们则以 $V(\chi)$ 或 $V \otimes \chi$ 记线性特征标 χ 对 V 的扭变: 这是一个由 $\rho_{V(\chi)}(g) = \chi(g)\rho_V(g)$ 定义的表示 (向量空间 $V(\chi)$ 是

空间 V, 但作用被 χ 扭变; 矩阵 $R_{V(\chi)}(g)$ 是 $R_V(g)$ 乘以 $\chi(g)$). 如果 $g \in G$, 我们有 $\chi_{V(\chi)}(g) = \chi(g)\chi_V(g)$.

习题 I.1.10. — 定义两个线性特征标的乘积 $\chi_1\chi_2$ 为 $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$. 证明具有这个乘积的 $\widehat{G}$ 是个交换群.

习题 I.1.11. — (线性特征标的正交性)

(i) 设 G 为有限群, $\chi \in \widehat{G}$. 证明 $\frac{1}{|G|}\sum_{g\in G}\chi(g)$ 在 χ 为平凡特征标时取值为 1, 其他情形为 0.(以 $\chi(h)$ 乘此和, 其中 $h \in G$ 为一个适当选取的元.)

(ii) 由此推导出, 如果 $\chi_1, \chi_2 \in \widehat{G}$, 且 $\langle\chi_1, \chi_2\rangle = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_1(g)}\chi_2(g)$, 则当 $\chi_1 = \chi_2$ 时 $\langle\chi_1, \chi_2\rangle = 1$, 而当 $\chi_1 \neq \chi_2$ 时 $\langle\chi_1, \chi_2\rangle = 0$.

2.2. *直和*

如果 V_1 和 V_2 是 G 的两个表示, 我们可以给这两个向量空间 V_1 和 V_2 的直和 $V_1 \oplus V_2$ 一个 G 的作用. 我们知道 $V_1 \oplus V_2$ 是以 V_1 和 V_2 为子空间的一个向量空间并且 $V_1 \oplus V_2$ 是它们的直和. 由于我们做的是有限个空间的直和, 故 $V_1 \oplus V_2$ 等同于乘积 $V_1 \times V_2$, 其中 $v_1 \in V_1$ 等同于 $(v_1, 0) \in V_1 \times V_2$, 而 $v_2 \in V_2$ 等同于 $(0, v_2) \in V_1 \times V_2$. 利用这些等同, $g \in G$ 在 $(v_1, v_2) \in V_1 \times V_2$ 的作用由 $g \cdot (v_1, v_2) = (g \cdot v_1, g \cdot v_2)$ 给出. 如此得到的 G 的表示仍旧记为 $V = V_1 \oplus V_2$, 并称其为 V_1 和 V_2 的*直和*. 如果 V_1 有一组基 $e_1, \ldots, e_m$ 和 V_2 有一组基 $f_1, \ldots, f_n$, 那么 $(e_1, 0), \ldots, (e_m, 0), (0, f_1), \ldots, (0, f_n)$ [237] 便是 V 的一组基, 在此基下矩阵 $R_V(g)$ 是分块对角矩阵 $\begin{pmatrix} R_{V_1}(g) & 0 \\ 0 & R_{V_2}(g) \end{pmatrix}$, 它的迹是 $R_{V_1}(g)$ 的迹与 $R_{V_2}(g)$ 的迹的和. 因此有

$$\chi_{V_1 \oplus V_2} = \chi_{V_1} + \chi_{V_2}.$$

这包括了 $V_1 = V_2 = V$ 的情形, 从而 $V \oplus V$ 是 G 的那样一个表示, 它包含了交为 0 而和为整个空间的两份 V. 例如, $\mathbf{Z}$ 的表示 $\mathbf{C}(\lambda) \oplus \mathbf{C}(\lambda)$ 是具有位似作用 λ 的 $\mathbf{C}^2$, 所得到的两份 $\mathbf{C}(\lambda)$ 是等同于乘积 $\mathbf{C} \times \{0\}$ 与乘积 $\{0\} \times \mathbf{C}$ 的直和 (因为任意一条直线都可以当作一份 $\mathbf{C}(\lambda)$, 故 $\mathbf{C}(\lambda)$ 有许多不同的方式进入到 $\mathbf{C}(\lambda) \oplus \mathbf{C}(\lambda)$ 中). 更一般地, 如果 $m \in \mathbf{N}$, 我们以 mV 记 m 份 V 的直和 (对于 $m = 0$, 得到的是向量空间 0). 如果这些 $V_i, i \in I$ 有限是 G 的表示, 而 $m_i \in \mathbf{N}$, $i \in I$, 则 $\oplus_{i\in I} m_i V_i$ 是 G 的一个表示, 它的特征标为

$$\chi_{\oplus_{i\in I} m_i V_i} = \sum_{i\in I} m_i \chi_{V_i}.$$

2.3. *置换表示, 正则表示*

如果 X 是一个有限集, 其上有一个 G 的 (左) 作用: $(g, x) \mapsto g \cdot x$. 定义与 X 相伴的一个*置换表示* V_X 为: V_X 是一个 $|X|$ 维的向量空间, 其基为 $(e_x)_{x\in X}$, 并具有 G 的线性作用: 在基的向量上 $g \cdot e_x = e_{g\cdot x}$. 对于 $g_1, g_2 \in G$ 及 $x \in X$, 我们

有 $g_1\cdot(g_2\cdot e_x)=g_1\cdot e_{g_2\cdot x}=e_{g_1g_2\cdot e_x}=g_1g_2\cdot e_x$, 这证明了上面的公式确实定义了 G 在 V_X 上的一个作用. 在基 $(e_x)_{x\in X}$ 下的 g 的矩阵是一个*置换矩阵* (即在每行每列上正好只有一个元 1 而其他系数均为 0 的矩阵), 并且对角项 $a_{x,x}$ 等于 1 当且仅当 $g\cdot x=x$(即 x 是 g 的不动点), 否则它为 0. 由此推导出 g 的迹是 g 作用在 X 上的不动点的个数. 换句话说, 我们有

$$\chi_{V_X}(g)=|\{x\in X, g\cdot x=x\}|.$$

特别令人感兴趣的一个情形是 G 有限而 $X=G$, G 的作用为左乘 (即 $g\cdot h=gh$). 如此得到的表示 V_G 便是 G 的*正则表示*. 由于 $gh=h$ 表明 $g=1$, 故我们可以看出正则表示的特征标由以下公式给出:

$$\chi_{V_G}(1)=|G|,\quad 而当\ g\in G-\{1\}\ 时\ \chi_{V_G}(g)=0.$$

习题 I.1.12. — 设 G 是作用于有限集 X 上的一个群. 证明, 如果 g,g' 在 G 中共轭, 则它们在 X 中的不动点的个数相同. 如何用 V_X 的特征标的语言来翻译它?

3. 表示的态射

3.1. 表示 Hom(V_1,V_2)

设 V_1 和 V_2 是 G 的两个表示, 而 $u:V_1\to V_2$ 是一个线性映射. 如果 $g\in G$, 定义 $g\cdot u:V_1\to V_2$ 为 $(g\cdot u)(v)=g\cdot u(g^{-1}\cdot v)$, 其中 $v\in V_1$. 如果 $g_1,g_2\in G$ 而 $v\in V_1$. 则有 [238]

$$\begin{aligned}(g_1\cdot(g_2\cdot u))(v)&=g_1\cdot((g_2\cdot u)(g_1^{-1}\cdot v))\\&=g_1\cdot(g_2\cdot u(g_2^{-1}\cdot g_1^{-1}\cdot v))\\&=g_1g_2\cdot u((g_1g_2)^{-1}\cdot v)\\&=(g_1g_2\cdot u)(v).\end{aligned}$$

因此 $g_1\cdot(g_2\cdot u)=g_1g_2\cdot u$, 这证明了我们定义了 G 在 V_1 到 V_2 的线性映射的空间 Hom(V_1,V_2) 上的一种作用.

如果 $g\in G$, 于是 Hom(V_1,V_2) 的自同态 $\rho_{\mathrm{Hom}(V_1,V_2),g}$ 便由公式

$$\rho_{\mathrm{Hom}(V_1,V_2),g}(u)=\rho_{V_2,g}\circ u\circ\rho_{V_1,g}^{-1},\ u\in\mathrm{Hom}(V_1,V_2)$$

定义.

命题 I.1.13. — *如果 G 有限, 且 $g\in G$, 则*

$$\chi_{\mathrm{Hom}(V_1,V_2)}(g)=\overline{\chi_{V_1}(g)}\chi_{V_2}(g).$$

证明 如果 g 是个固定元, 则可选取 V_1 的一组基 $(e_i)_{i\in I}$ 和 V_2 的一组基 $(f_j)_{j\in J}$, 使得在它们之下 g 的作用为对角的. 于是对于 $i\in I$ 存在 α_i, 对于 $j\in J$ 存在 β_j,

使得 $g\cdot e_i=\alpha_i e_i$, $i\in I$, 以及 $g\cdot f_j=\beta_j f_j$, $j\in J$. 因此 $\chi_{V_1}(g)=\sum_{i\in I}\alpha_i$ 和 $\chi_{V_2}(g)=\sum_{j\in J}\beta_j$.

如果 $(i,j)\in I\times J$, 并设 $u_{i,j}:V_1\to V_2$ 为由 $u_{i,j}(e_i)=f_j$ 和 $u_{i,j}(e_{i'})=0$, $i\neq i'$ 定义的一个线性映射. 对于 $(i,j)\in I\times J$ 的这些 $u_{i,j}$ 构成了 $\mathrm{Hom}(V_1,V_2)$ 的一组基, 而且有 $g\cdot u_{i,j}=\alpha_i^{-1}\beta_j u_{i,j}=\overline{\alpha_i}\beta_j u_{i,j}$. 所以我们有

$$\chi_{\mathrm{Hom}(V_1,V_2)}(g)=\sum_{(i,j)\in I\times J}\overline{\alpha_i}\beta_j=(\sum_{i\in I}\overline{\alpha_i})(\sum_{j\in J}\beta_j)=\overline{\chi_{V_1}(g)}\chi_{V_2}(g).$$

得到了结论. □

注记 I.1.14. — 如果 $V_1=V$, 而 V_2 是平凡表示, 则表示 $\mathrm{Hom}(V_1,V_2)=\mathrm{Hom}(V,\mathbf{C})$ 是 V 的对偶表示 V^*. 于是根据命题 I.1.13 有 $\chi_{V^*}=\overline{\chi_V}$.

3.2. 交叉算子, 表示的同构

以 $\mathrm{Hom}_G(V_1,V_2)$ 记 V_1 到 V_2 的那些与 G 的作用交换的线性映射. 它是 $\mathrm{Hom}(V_1,V_2)$ 中的一个向量子空间, 而 $\mathrm{Hom}(V_1,V_2)$ 中的一个元 u 属于 $\mathrm{Hom}_G(V_1,V_2)$ 当且仅当对任意的 $v\in V_1$, $g\in G$ 有 $g\cdot u(v)=u(g\cdot v)$. 应用到 $g^{-1}\cdot v$, 这也可以重写为对任意的 $v\in V_1$ 有 $g\cdot u(g^{-1}\cdot v)=u(v)$, 或者再写成 $g\cdot u=u$ 的形式. 即 $\mathrm{Hom}_G(V_1,V_2)$ 是 $\mathrm{Hom}(V_1,V_2)$ 在 G 作用下的不动元的向量子空间. 常常称 $\mathrm{Hom}_G(V_1,V_2)$ 中的元为交叉算子.

例题 I.1.15. — 如果 V 是 G 的一个表示, V 中在 G 作用下的不动元的集合 V^G 是 V 的一个向量子空间 (它是对于 $g\in G$ 的 $g-1$ 的核的交), 它在 G 的作用下稳定, 并且 G 在其上的作用按构造是平凡的, 因此是 G 的一个表示. 现在, 如果 G 有限, 我们则可以考虑平均算子 $M:V\to V$, 其定义为 $M(v)=\frac{1}{|G|}\sum_{g\in G}g\cdot v$. M 是 V 和 V^G 之间的一个交叉算子. 事实上, 如果 $h\in G$, $v\in V$, 我们则有 [239]

$$h\cdot M(v)=h\cdot\left(\frac{1}{|G|}\sum_{g\in G}g\cdot v\right)=\frac{1}{|G|}\sum_{g\in G}h\cdot(g\cdot v)=\frac{1}{|G|}\sum_{g\in G}g\cdot v,$$

$$M(h\cdot v)=\frac{1}{|G|}\sum_{g\in G}g\cdot(h\cdot v)=\frac{1}{|G|}\sum_{g\in G}gh\cdot v,$$

并且因为 $g\mapsto hg$ 和 $g\mapsto gh$ 都是 G 到 G 的双射, 故这两个都等于 $M(v)$. 这同时证明了 $M(v)\in V^G$ 和 $M:V\to V^G$ 与 G 的作用交换.

注记 I.1.16. — 为了得到整个群作用下的不变的某些东西只要考虑这个平均算子就可以了这个想法在表示论中起着极其重要的作用.

我们说 G 的两个表示 V_1 和 V_2 是同构的是指存在一个与 G 的作用交换的线性同构 $u:V_1\to V_2$ (换句话说存在一个双射 $u\in\mathrm{Hom}_G(V_1,V_2)$, 特别地, 这表明 V_1 和 V_2 有相同的维数). 用与 V_1 和 V_2 相关的同态 $\rho_{V_1}:G\to\mathrm{GL}(V_1)$ 和 $\rho_{V_2}:G\to\mathrm{GL}(V_2)$

的语言翻译过来, 这个关系变成 $u \circ \rho_{V_1}(g) = \rho_{V_2}(g) \circ u$, 其中任意 $g \in G$. 用矩阵的语言翻译 (在选取了 V_1 和 V_2 的基之后) 便成为: 存在 $T \in \mathbf{GL}_d(\mathbf{C})$ 使得对于任意的 $g \in G$ 有 $TR_{V_1}(g) = R_{V_2}(g)T$, 这又可以写为形式 $R_{V_2}(g) = TR_{V_1}(g)T^{-1}$. 特别地, 对于任意的 $g \in G$ 有 $\chi_{V_1}(g) = \chi_{V_2}(g)$.

习题 I.1.17. — 给出 $\mathbf{Z}/2\mathbf{Z}$ 的两个有相同维数但却不同构的表示.

注记 I.1.18. — (i) 我们将在后面看到, 如果 G 有限, 则上面最后断言的逆也成立: 如果 V_1 和 V_2 具有相同的特征标, 则它们同构, 这似乎多少有点令人惊讶, 因为特征标仅仅由计算自同态的迹得到. 下面的习题 I.1.19 使得这个结果能够预想到.

(ii) 在 $\mathbf{Z}$ 的情形, 对于 $i = 1, 2$ 以 R_i 记 $\rho_{V_i}(1)$ 的矩阵, 我们看到 V_1 与 V_2 同构当且仅当存在可逆的 T 使得 $R_2 = TR_1T^{-1}$ (即当且仅当 R_2 和 R_1 为相似矩阵), 由此得到 $\mathbf{Z}$ 的表示在同构意义下的分类等价于矩阵在相似意义下的分类, 这可利用若尔当形式来做. 如果我们让 $R = R_V(1)$ 是可对角化的, 那么 V 在同构意义下由 R 的带重数的特征值给出.

习题 I.1.19. — 设 V 是有限群 G 的一个表示. 如果 $g \in G$, 并令 $P_g(T) = \det(1 - T\rho_V(g))$. 证明成立形式级数的恒等式 $-\sum_{n=0}^{+\infty} \chi_V(g^{n+1})T^n = \frac{P_g'(T)}{P_g(T)}$. 由此推导出, 对于任意的 $g \in G$, χ_V 可以在差一个 $GL(V)$ 中的元的共轭下确定 $\rho_V(g)$.

I.2. 表示的分解 [240]

当我们试图对某种类型的对象进行分类时 (譬如有限群、有限群的表示 $\cdots\cdots$), 就会被引导去了解那些不能进一步分成更小的对象 (在群情形中的单群、在有限群的表示情形中的不可约表示 $\cdots\cdots$), 以及如何由这些小对象拼装起来以描述那些让我们感兴趣的整个对象. 在有限群的表示情形中, 马什克 (Maschke) 定理 (定理 I.2.7) 证明了上述第二步是完全可行的; 同时, 推论 I.2.16 表明要列出所有不可约对象并不是一件不可企及的事.

1. 分解为不可约表示的直和

设 G 为群, V 是 G 的一个表示. V 的一个子表示是 V 的一个在 G 下稳定的子空间. 譬如, 如果 $v \in V - \{0\}$, V 中由 $g \cdot v$, $g \in G$ 生成的子空间是 V 的一个子表示; 称它为由 v 生成的 V 的子表示 (即 V 的包含 v 的最小子表示). 称 V 是不可约的是说 V 除去 0 和 V 外它没有其他的子表示. 一个等价的说法是, V 为不可约是说对于任意的 $v \in V - \{0\}$, 由对所有 $g \in G$ 的 $g \cdot v$ 生成的 V 的子空间等于 V 自己.

例题 I.2.1. — 习题 I.1.6 中的 S_3 在 $\mathbf{C}^2$ 上的那个表示是不可约的. 事实上, 由于它的维数等于 2, 在 0 和 $\mathbf{C}^2$ 外的子表示应是 $\mathbf{C}^2$ 的一条直线. 这样一条直线特别地应该在相对于 (OA) 和 (OB) 的正交对称环 s_{OA} 和 s_{OB} 下稳定, 由于这种在 s_{OA} 下稳

定的直线必是坐标轴, 但这些坐标轴却在 s_{OB} 下不稳定, 故这是不可能的.

习题 I.2.2. — 设 S_3 为集合 $\{1,2,3\}$ 的置换群, 而 s 和 t 是 S_3 的元 (12) 和 (123).

(i) 令 s 和 t 为 S_3 中的元 (12) 和 (123). 验证 (或承认) s 和 t 生成了 S_3 且 $sts^{-1}=t^2$; 确定 S_3 的共轭类.

(ii) 设 V 是 S_3 的一个有限维表示, 且 W_0, W_1 和 W_2 是 t 的 (即 $\rho_V(t)$ 的) 对应于特征值 $1, j=e^{2i\pi/3}$ 和 j^2 的特征空间. 证明 $V=W_0\oplus W_1\oplus W_2$.

(iii) 证明 W_0 在 s 下稳定, 而 s 交换 W_1 和 W_2.

(iv) 证明, 如果 $v\in W_1-\{0\}$, 则有 v 和 $s\cdot v$ 生成的 V 的子空间在 S_3 下稳定, 并且作为 S_3 的表示是不可约的, 而如此得到的表示不依赖 (在同构意义下)v 的选取.

(v) 由此推导出 V 有一个 S_3 的不可约表示和的分解以及 S_3 的一个不可约表示的列表.

例题 I.2.3. — 设 V 是 $\mathbf{Z}$ 的一个表示, 且 $u=\rho_V(1)$, 由于 $\mathbf{C}$ 是代数闭的, 且因 u 可逆, 故 u 有一个非零的特征值 λ. 令 $e_\lambda\in V$ 为对应特征值 λ 的特征向量. 于是有 $n\cdot e_\lambda=u^n(e_\lambda)=\lambda^n e_\lambda$, 其中任意 $n\in\mathbf{N}$, 这证明了直线 $\mathbf{C}e_\lambda$ 在 $\mathbf{Z}$ 的作用下稳定, 从而是一个同构于习题 I.1.2 中的表示 $\mathbf{C}(\lambda)$ 的一个子表示. 特别地, 如果 V [241] 的维数 $\geqslant 2$, 则 V 不是不可约的, 因此 $\mathbf{Z}$ 的所有不可约表示的维数都是 1, 同构于被 $\lambda\in\mathbf{C}^*$ 唯一确定的 $\mathbf{C}(\lambda)$.

现假设 u 为可对角化的. 设 $e_1,\ldots,e_d$ 为 u 的特征向量构成的 V 的一组基, 而 λ_i 是对应于 e_i 的特征值. 于是 V 是 V 的子表示即直线 $\mathbf{C}e_i$ 的直和 $\oplus_{i=1}^d\mathbf{C}e_i$, 同构于 $\mathbf{C}(\lambda_i)$ 的每个 $\mathbf{C}e_i$ 是 $\mathbf{Z}$ 的表示. 由此推导出作为 $\mathbf{Z}$ 的表示的 V 同构于 $\oplus_{i=1}^d\mathbf{C}(\lambda_i)$.

注记 I.2.4. — (i) 说 V 同构于 $\oplus_{i=1}^d\mathbf{C}(\lambda_i)$ 意味着 $u=\rho_V(1)$ 是可对角化的, 其特征多项式为 $\prod_{i=1}^d(X-\lambda_i)$, 它比起给出一组以特征向量组成的基更不准确, 它只是 $\mathbf{Z}$ 的表示 $\oplus_{i=1}^d\mathbf{C}(\lambda_i)$ 到 V 之间的一个同构.

(ii) 如果 u 是可对角化的, 且 u 的特征值为 $\lambda_1,\ldots,\lambda_r$, 当 $i\neq j$ 时 $\lambda_i\neq\lambda_j$, 而 λ_i 的重数为 m_i, 则 $V\cong\oplus_{i=1}^r m_i\mathbf{C}(\lambda_i)$.

(iii) 如果 u 不是可对角化的, 表示 V 便不能分解为不可约表示的直和.

习题 I.2.5. — 设 η 是 G 的一个线性特征标. 证明, 对于 G 的所有不可约表示 V, 表示 $V\otimes\eta$ 仍是不可约的.

我们要证明, *如果 G 是有限的*, 则 G 的所有表示均是不可约表示的直和. 对这些不可约表示中的每个选取一组基等于给出了 V 的一组基, 在此基下 $\rho_V(g)$, $g\in G$ 同

时按分块取对角形式[4], 而且这些块矩阵是最小的. (这有点类似于 $\mathbf{R}^n$ 中一个旋转矩阵的最小形式.) 我们将来需要以下结果.

定理 I.2.6. — *设 V 是 G 的一个表示. 则在 V 上存在一个在 G 下不变的标量积 $\langle,\rangle_V$.*

证明 从任意一个标量积 $\langle,\rangle$ 着手, 并定义 $\langle,\rangle_V$ 为 $\langle,\rangle$ 在 G 作用下的变换的平均. 换而言之,

$$\langle v_1, v_2\rangle_V = \frac{1}{|G|}\sum_{g\in G}\langle g\cdot v_1, g\cdot v_2\rangle.$$

G 的作用的线性性导致了它对于 v_2 的线性和对于 v_1 的半线性. 另外, $\langle v,v\rangle_V \geqslant \frac{1}{|G|}\langle v,v\rangle$ 证明了 $\langle,\rangle_V$ 是正定的. 最后, 如果 $h\in G$, 那么我们有 [242]

$$\langle h\cdot v_1, h\cdot v_2\rangle_V = \frac{1}{|G|}\sum_{g\in G}\langle g\cdot(h\cdot v_1), g\cdot(h\cdot v_2)\rangle = \frac{1}{|G|}\sum_{g\in G}\langle gh\cdot v_1, gh\cdot v_2\rangle = \langle v_1, v_2\rangle_V,$$

其中 $g\mapsto gh$ 诱导了 G 自身的一个双射. 故得结论. □

定理 I.2.7. — (马什克 (Maschke), 1899) *G 的所有表示都是不可约表示的直和.*

证明 证明由对维数的归纳进行. 如果 V 为 1 维的或者说是不可约的, 则无需做什么. 如果 V 的维数 $\geqslant 2$, 并不是不可约的, 则 V 具有一个不同于 0 和 V 的子表示 V_1. 如果 $\langle,\rangle_V$ 是在 V 上的一个在 G 的作用下不变的标量积, 那么 V_1 的正交补 V_2 也在 G 下不变, 这是因为由此标量积的不变性得到 "v 正交于 V_1" 等价于 "$g\cdot v$ 正交于 $g\cdot V_1 = V_1$". 因此我们有 $V = V_1\oplus V_2$, 而 V_1 和 V_2 的维数都严格小于 V 的维数. 归纳假设让我们得到作为不可约表示的直和分解, 从而证明了 V 同样有这样的分解. □

注记 I.2.8. — 如果 G 是由 g 生成的循环群, V 的不可约表示和的分解等价于 V 的一个在 g 作用下不变的直线的分解. 我们已知, 如果 g 有一个重数 >1 的特征值, 那么这个分解不是唯一的. 另外, 分解为特征子空间时它却是完全典范的. 我们在后面将看到 (推论 I.2.20), 这种情形在分解任意一个有限群的表示为不可约表示和时同样也成立.

2. 舒尔引理及其直接推论

定理 I.2.9. — (舒尔 (Schur) 引理, 1905) *设 G 为有限群, V_1 和 V_2 为 G 的不可约*

[4]这对于特征为 0 的域上的有限群的表示来说, 是十分特别的. 让我们考虑在一个特征 >0 的域上的有限群的情形, 我们期望最好能得到的是一个分块取上三角的形式. 举例来说, 如果 V 是在域 $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ 上的 $G=\mathbf{Z}/p\mathbf{Z}$ 的一个 2 维表示, $n\in\mathbf{N}$ 在基 (e_1,e_2) 下的矩阵是 $\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}$, 于是由 e_1 生成的子空间 V_1 在 G 下稳定 (且不动), 但容易看出这是 V 的具有这个性质的唯一的特征空间. 表示 V 因此不是不可约的, 也不是不可约表示的直和.

表示,

(i) 如果 V_1 和 V_2 不同构, 则 $\mathrm{Hom}_G(V_1, V_2) = 0$.

(ii) 如果 $V_1 = V_2$, 则 $\mathrm{Hom}_G(V_1, V_2)$ 中的元是一条位似直线.

证明　设 $u \in \mathrm{Hom}_G(V_1, V_2)$, u 与 G 的作用交换的性质表明 $\mathrm{Ker}(u) \subset V_1$ 和 $\mathrm{Im}(u) \subset V_2$ 在 G 作用下稳定. 按假定条件, V_1 与 V_2 不可约, 故而或是 $\mathrm{Ker}(u) = V_1$, 这时 $u = 0$; 或是 $\mathrm{Ker}(u) = 0$, 这时 $\mathrm{Im}(u) \neq 0$, 从而 $\mathrm{Im}(u) = V_2$. 于是由此得知, 如果 $u \neq 0$, 则 u 同时为单射 (因为 $\mathrm{Ker}(u) = 0$) 和满射, 于是是个同构. (i) 得证.

转向 (ii). 由于我们处理的是 $\mathbf{C}$-向量空间, 故 u 有特征值 λ. 因为 u 与 G 的作用交换并且位似映射也如此, 故 $u - \lambda$ 也如此. 与 (i) 同样的推理证明它的核应该等于 V_1, 这等于说 u 是具比率 λ 的位似变换. 证完. □

[243]

注记 I.2.10. — 如果 V_1 和 V_2 仅为空间的同构, 而 $u : V_1 \to V_2$ 是一个表示间的同构, 那么从舒尔引理的 (ii) 得知, $\mathrm{Hom}_G(V_1, V_2)$ 的每个元都具有 λu, $\lambda \in \mathbf{C}$ 的形式.

习题 I.2.11. — 设 G 为交换群. 证明 G 的每个不可约表示的维数均为 1.

命题 I.2.12. — 设 G 为有限群而 V_1, V_2 为 G 的表示.

(i) 如果 V_1 和 V_2 不可约但不同构, 而 $u \in \mathrm{Hom}(V_1, V_2)$, 则

$$M(u) = \frac{1}{|G|} \sum_{g \in G} g \cdot u = 0.$$

(ii) 如果 V 不可约, 而 $u \in \mathrm{Hom}(V, V)$, 则 $M(u) = \frac{1}{|G|} \sum_{g \in G} g \cdot u$ 是比率为 $\frac{1}{\dim V} \mathrm{Tr}(u)$ 的位似.

(iii) 如果 V 不可约, 而 ϕ 是 G 上的一个中心函数, 则 $\sum_{g \in G} \phi(g) \rho_V(g)$ 是一个比率为 $\frac{1}{\dim V} \sum_{g \in G} \phi(g) \chi(g)$ 的位似.

证明　如果 V_1 和 V_2 是 G 的两个表示, 且 $u \in \mathrm{Hom}(V_1, V_2)$, 而如果 $h \in G$, 于是我们有 $h \cdot (\sum_{g \in G} g \cdot u) = \sum_{g \in G} hg \cdot u$. 由于 $g \mapsto hg$ 是 G 到自己的一个双射, 这最后的项也等于 $\sum_{g \in G} g \cdot u$. 因此得到 $M(u) = \frac{1}{|G|} \sum_{g \in G} g \cdot u$ 属于 $\mathrm{Hom}_G(V_1, V_2)$.

那么 (i) 就是舒尔引理的 (i) 的推论. 然而舒尔引理的 (ii) 证明了, 如果 $u \in \mathrm{Hom}(V, V)$ 且 V 不可约, 则 $M(u)$ 是个位似映射. 为了确定这个位似的比率, 只要计算它的迹并除以 $\dim V$ 即可. 然而我们有 $M(u) = \frac{1}{|G|} \sum_{g \in G} \rho_V(g) u \rho_V(g)^{-1}$, 从而 $M(u)$ 是 $|G|$ 个项的平均, 而由于迹在共轭下不变, 故每个项的迹都为 $\mathrm{Tr}(u)$. 因此我们有 $\mathrm{Tr}(M(u)) = \mathrm{Tr}(u)$, (ii) 得证.

最后, 如果 ϕ 是一个中心函数 (即对于所有 $h, g \in G$, $\phi(hgh^{-1}) = \phi(g)$), 且如果 $u_\phi = \sum_{g \in G} \phi(g) \rho_V(g) \in \mathrm{Hom}(V, V)$, 而 $h \in G$. 我们则有

$$\begin{aligned} h \cdot u_\phi = \rho_V(h)(\sum_{g \in G} \phi(g) \rho_V(g)) \rho_V(h)^{-1} &= \sum_{g \in G} \phi(g) \rho_V(hgh^{-1}) \\ = \sum_{g \in G} \phi(hgh^{-1}) \rho_V(hgh^{-1}) &= \sum_{g \in G} \phi(g) \rho_V(g) = 0 = u_\phi. \end{aligned}$$

像上面那样我们得到 u_ϕ 是一个位似, 其比率为

$$\frac{1}{\dim V}\mathrm{Tr}(u_\phi) = \frac{1}{\dim V}\sum_{g\in g}\phi(g)\mathrm{Tr}(\rho_V(g)) = \frac{1}{\dim V}\sum_{g\in G}\phi(g)\chi_V(g).$$

证完. □

3. 特征标的正交性

[244]

设 G 为有限群. 以 $R_{\mathbf{C}}(G)$ 记中心函数构成的向量空间. 这个空间包含了 G 自己的表示的特征标的集合 $R^+(G)$, 还包含了 G 的不可约特征标的集合 $\mathrm{Irr}(G)$(即 G 的不可约表示的特征标的集合). 最后, 以 $R_{\mathbf{Z}}$ 记 G 的伪特征标的集合; 这是由 $R^+(G)$ 生成的 $R_{\mathbf{C}}(G)$ 的 (加法) 子群.

习题 I.2.13. — 证明 $R^+(G)$ 在加法下稳定, 而 $R_{\mathbf{Z}}(G)$ 是对所有 $\chi_1, \chi_2 \in R^+(G)$ 的 $\chi_1 - \chi_2$ 的集合.

我们在 $R_{\mathbf{C}}(G)$ 上给予一个标量积 $\langle , \rangle$, 其定义为

$$\langle \phi_1, \phi_2 \rangle = \frac{1}{|G|}\sum_{g\in G}\overline{\phi_1(g)}\phi_2(g).$$

定理 I.2.14. — (弗罗贝尼乌斯 (Frobenius), 1897) *不可约特征标构成了中心函数空间的一族法正交基.*

证明 设 χ_1, χ_2 为两个特征标, 而 V_1, V_2 是 G 的两个其特征标分别为 χ_1, χ_2 的表示. 利用命题 I.1.13, 可以重写 $\langle \chi_1, \chi_2 \rangle$ 为形式

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_1(g)}\chi_2(g) = \frac{1}{|G|}\sum_{g\in G}\chi_{\mathrm{Hom}(V_1,V_2)}(g).$$

由于按定义, $\chi_{\mathrm{Hom}(V_1,V_2)}(g)$ 是 g 作用在 $\mathrm{Hom}(V_1, V_2)$ 上的迹, 这让我们可将 $\langle \chi_1, \chi_2 \rangle$ 看成是在命题 I.2.12 中定义的线性映射 $u \mapsto \frac{1}{|G|}\sum_{g\in G} g\cdot u = M(u)$ 的迹, 从这个命题的 (i) 和 (ii) 可推导出如下的事实:

- 如果 χ_1 和 χ_2 不可约且不相等, 则 M 恒为 0, 从而 $\langle \chi_1, \chi_2 \rangle = \mathrm{Tr}(M) = 0$.
- 如果 χ 不可约, 且 V 是一个特征标为 χ 的表示, 则 M 是与 $u \in \mathrm{Hom}(V, V)$ 相伴的比率为 $\frac{1}{\dim V}\mathrm{Tr}(u)$ 的位似映射. 因此得知, 当 M 的特征值为 1 时, 重数为 1, 对应的特征空间是一条位似直线; 而当为 0 时, 重数为 $(\dim V)^2 - 1$, M 的核是一个迹为 0 的自同态的超平面. 因此 M 的迹为 1, 也就是说 $\langle \chi, \chi \rangle = 1$.

从上面的这两个事实得到这些不可约特征标形成了一个法正交族. 还需证明它是 $R_{\mathbf{C}}(G)$ 的基, 为此只需证明一个中心函数 ϕ 若与 $\mathrm{Irr}(G)$ 的所有元正交, 则必为零即可. 那么, 考虑 G 的正则表示 V_G, 并设 $V_1 \oplus \cdots \oplus V_r$ 是它的不可约分解. 如果 ϕ 是一个与 χ_{V_i} 正交的中心函数, 由命题 I.2.12 的 (iii) 得到 V_i 的自同态 $\sum_{g\in G}\overline{\phi(g)}\rho_{V_i}(g)$ 为

[245] 零. 因此, 如果 ϕ 正交于所有这些不可约特征标, 则 V_G 的自同态 $\sum_{g\in G}\overline{\phi(g)}\rho_{V_G}(g)$ 为零. 将这个自同态作用在 $e_1\in V_G$ 上, 由此便得到 $0=\sum_{g\in G}\overline{\phi(g)}g\cdot e_1=\sum_{g\in G}\overline{\phi(g)}e_g$. 然而这些 e_g, 其中 $g\in G$, 构成了 V_G 的一组基; $\sum_{g\in G}\overline{\phi(g)}e_g$ 为零表明对于任意的 g 的 $\overline{\phi(g)}$ 为零, 从而 ϕ 为零. 得证. □

注记 I.2.15. — 如果 V_1 和 V_2 不可约且互不同构, 那么映射 M 恒等于零从而 $\mathrm{Tr}(M)=0$. 然而从定理 I.2.14 的证明得知 $\mathrm{Tr}(M)=\langle\chi_{V_1},\chi_{V_2}\rangle$. 于是由此特别得到 $\chi_{V_1}\neq\chi_{V_2}$. 换而言之, 映射 $W\mapsto\chi_W$ 是从 G 的不可约表示的集合 (在同构意义下) 到 $\mathrm{Irr}(G)$ 的单射. 由于按 $\mathrm{Irr}(G)$ 的定义, 这个映射为满射, 故为双射. 这让我们将 $\mathrm{Irr}(G)$ 也看作 G 的不可约表示的集合. 对 $\mathrm{Irr}(G)$ 的这个解释将在下文中用到.

4. 主定理的应用

定理 I.2.14 有一系列漂亮的应用.

4.1. 不可约表示的个数

推论 I.2.16. — *G 的不可约表示的个数等于 G 中共轭类的个数 $|\mathrm{Conj}(G)|$. 特别地, 它是有限的.*

证明　根据定理 I.2.14, G 的不可约表示的个数等于中心函数空间 $R_{\mathbf{C}}(G)$ 的维数. 而一个函数是中心函数当且仅当它在每个共轭类上为常值; 于是一个中心函数 ϕ 可以唯一地写成 $\phi=\sum_{C\in\mathrm{Conj}(G)}\lambda_C\mathbf{1}_C$ 形式, 其中 $\mathbf{1}_C$ 是 C 的特征函数, 而 $\lambda_C\in\mathbf{C}$(有 $\lambda_C=\phi(g)$, g 为 C 的任意元). 这些 $\mathbf{1}_C$, 其中 $C\in\mathrm{Conj}(G)$, 形成了 $R_{\mathbf{C}}(G)$ 的一组基, 由此事实知它的维数为 $|\mathrm{Conj}(G)|$. 得证. □

注记 I.2.17. — G 的不可约表示的集合和 G 的共轭类的集合具有相同的基数, 但一般说来, 不存在这两个集合之间的自然的双射. 对称群却构成了一个令人瞩目的例外 (参看 C.2 小节).

4.2. 表示的典范分解

下面的结果有点神秘但非常有用 (譬如用 §I.3 的 2 小节的张量方法去分解得到的表示, 这在粒子物理中经常使用); 我们能够将它看作从特征多项式去计算一个自同态的特征值方法的推广. 在这两种情形我们都无意于显式地给出这些具有好性质的向量; 我们仅满足于证明它的存在性.

[246] **推论 I.2.18.** — *如果 V 是 G 的一个表示, 而 $V=W_1\oplus\cdots\oplus W_k$ 是 V 的一个不可约表示的直和分解, 并且如果 $W\in\mathrm{Irr}(G)$, 那么同构于 W 的这些 W_i 的个数 m_W 等于 $\langle\chi_W,\chi_V\rangle$. 特别地, 它不依赖这个分解, 且 $V\cong\oplus_{W\in\mathrm{Irr}(G)}\langle\chi_W,\chi_V\rangle W$.*

证明　我们有 $\chi_V=\chi_{W_1}+\cdots+\chi_{W_k}$, 故

$$\langle\chi_W,\chi_V\rangle=\langle\chi_W,\chi_{W_1}\rangle+\cdots+\langle\chi_W,\chi_{W_k}\rangle.$$

然而 $\langle \chi_W, \chi_{W_i} \rangle$ 为 0 还是 1 按照 W_i 是否同构于 W 而定; 因此有 $\langle \chi_W, \chi_V \rangle = m_W$. 于是得到了结论. □

推论 I.2.19. — G 的两个表示 V_1 和 V_2 如果具有同一个特征标 χ, 则同构.

证明 根据推论 I.2.18, 它们两个全都同构于 $\oplus_{W\in \mathrm{Irr}(G)} \langle \chi_W, \chi \rangle W$. □

推论 I.2.20. — (将表示分解为同型 (isotypique) 的分支) 如果 V 是 G 的一个表示, 且 $W \in \mathrm{Irr}(G)$, 则

$$p_W = \frac{\dim W}{|G|} \sum_{g\in G} \overline{\chi_W(g)} \rho_V(g)$$

是一个与 G 的作用交换的投射算子. 另外, G 的所有出现在 $p_W(V)$ 的分解中的不可约表示均同构于 W, 而 V 是这些 $p_W(V)$ 的直和, 其中 $W \in \mathrm{Irr}(G)$.

证明 如果 $V = W_1 \oplus \cdots \oplus W_k$ 是 V 的不可约表示的直和分解. 根据命题 I.2.12, p_W 在 W_i 上的限制是个比率为

$$\frac{\dim W}{|G| \dim W_i} \sum_{g\in G} \overline{\chi_W(g)} \chi_{W_i}(g) = \frac{\dim W}{\dim W_i} \langle \chi_W, \chi_{W_i} \rangle$$

的位似. 按照特征标的正交性的关系, 这表明当 $W \cong W_i$ 时 p_W 在 W_i 上为恒等, 而在其他情形为零. 由此导出结果. □

4.3. 不可约性的一个判别准则

推论 I.2.21. — G 的一个表示 V 不可约当且仅当 $\langle \chi_V, \chi_V \rangle = 1$.

证明 如果 $V \cong \oplus_{W\in \mathrm{Irr}(G)} m_W W$, 则

$$\langle \chi_V, \chi_V \rangle = \langle \sum_{W\in \mathrm{Irr}(G)} m_W \chi_W, \sum_{W\in \mathrm{Irr}(G)} m_W \chi_W \rangle = \sum_{W\in \mathrm{Irr}(G)} m_W^2.$$

由于 m_W 是自然数, 故得到 $\langle \chi_V, \chi_V \rangle = 1$ 当且仅当出了一个 m_W 等于 1 外其余全为 0. 得证. □

习题 I.2.22. — 设 $\chi \in R_{\mathbf{Z}}(G)$. 证明下面的条件等价: [247]

(i) $\chi \in \mathrm{Irr}(G)$.

(ii) $\langle \chi, \chi \rangle = 1$, 且 $\chi(1) \geqslant 0$.

4.4. 正则表示的分解

推论 I.2.23. — (i) 如果 W 不可约, 则 W 以重数 $\dim W$ 出现在 G 的正则表示中.

(ii) 有 $\sum_{W\in \mathrm{Irr}(G)} (\dim W)^2 = |G|$ (伯恩赛德 (Burnside) 公式 [5]).

(iii) 如果 $g \neq 1$, 则 $\sum_{W\in \mathrm{Irr}(G)} \dim W \chi_W(g) = 0$.

---

[5] 在 S_n 的情形我们将给出这个公式的直接证明, 参看附录 C 的注 (2).

证明　正则表示的特征标 χ_{V_G} 由 $\chi_{V_G}(1)=|G|$, 而当 $g\neq 1$ 时 $\chi_{V_G}(g)=0$ 给出 (§I.1 的 2.3 节). 但 W 在 V_G 中的重数, 按照推论 I.2.18, 等于

$$\langle\chi_W,\chi_{V_G}\rangle=\frac{1}{|G|}\sum_{g\in G}\overline{\chi_W(g)}\chi_{V_G}(g)=\frac{1}{|G|}\overline{\chi_W(1)}|G|=\overline{\chi_W(1)}=\dim W.$$

这证明了 (i). 由此得到 $\chi_{V_G}=\sum_{W\in\mathrm{Irr}(G)}\dim W\chi_W$. 将此应用于恒等式 $g=1$, 则得到了 (ii), 而应用到 $g\neq 1$ 则推导出了 (iii). □

5. 交换群的情形

5.1. 傅里叶变换

定理 I.2.24. — 如果 G 为交换的, 则 G 的每个不可约表示的维数为 1. 换而言之, $\mathrm{Irr}(G)$ 与 G 的线性特征标的集合 $\widehat{G}$ 相等.

证明　如果 G 为交换的, 从而它的共轭类都化成单个元, 故 $|\mathrm{Conj}(G)|=|G|$. 根据推论 I.2.16 知 $|\mathrm{Irr}(G)|=|\mathrm{Conj}(G)|$, 但由推论 I.2.23 有 $\sum_{W\in\mathrm{Irr}(G)}(\dim W)^2=|G|$, 并由于对于任意的 $W\in\mathrm{Irr}(G)$ 有 $\dim W\geqslant 1$, 故得到对于任意的 $W\in\mathrm{Irr}(G)$ 有 $\dim W=1$. 得证[6]. □

推论 I.2.25. — 如果 G 为交换的, 则每个从 G 到 $\mathbf{C}$ 的函数是线性特征标的线性组合.

证明　根据定理 I.2.14, 每个中心函数 (因为 G 为交换的, 即为每个函数) 是不可约特征标的线性组合. 于是定理 I.2.24 给出了结论. □

由于一个交换群 G 的线性特征标构成了 G 到 $\mathbf{C}$ 的函数的正交基, 那么很容易将 [248] 任意一个函数分解为线性特征标的线性组合. 如果 ϕ 是 G 上的一个函数, 定义它的傅里叶变换 $\hat{\phi}$ 为在 $\widehat{G}$ 上由

$$\hat{\phi}(\chi)=\langle\chi,\phi\rangle=\frac{1}{|G|}\sum_{g\in G}\overline{\chi(g)}\phi(g)=\frac{1}{|G|}\sum_{g\in G}\chi(g)^{-1}\phi(g)$$

定义的函数.

因此傅里叶反演公式可以表达为

$$\phi=\sum_{\chi\in\widehat{G}}\hat{\phi}(\chi)\chi;$$

这是这些 χ, $\chi\in\widehat{G}$ 是一族正交基的性质的直接推论. 举例来说, 如果应用上面的推论到函数 $\phi_a:G\to\mathbf{C}$, 它在 a 取值为 1, 其余取 0, 那么便有 $\hat{\phi}_a(\chi)=\frac{1}{|G|}\overline{\chi}(a)$, 从而得到

$$\frac{1}{|G|}\sum_{\chi\in\widehat{G}}\overline{\chi(a)}\chi(x)=\begin{cases}1, & \text{如果 } x=a,\\ 0, & \text{其他.}\end{cases}$$

---

[6] 在习题 I.1.8 和 I.2.11 中给出了更为平易的证明.

称群 $(\mathbf{Z}/D\mathbf{Z})^*$ 的一个线性特征标为 mod D 的狄利克雷特征标[39]. 以 $\mathrm{Dir}(D)$ 记这些特征标的集合. 下面的结果是关于算术级数的狄利克雷定理的证明 (参看定理 VII.4.7) 的组成部分.

命题 I.2.26. — 如果 a 与 D 互素, 则

$$\frac{1}{\varphi(D)}\sum_{\chi\in\mathrm{Dir}(D)}\overline{\chi(a)}\chi(n)=\begin{cases}1, & \text{如果 } n\equiv a \bmod D,\\ 0, & \text{其他.}\end{cases}$$

证明 将上面的结果应用于群 $(\mathbf{Z}/D\mathbf{Z})^*$, 该群基数为 $\varphi(D)$, 函数 $\phi_a:(\mathbf{Z}/D\mathbf{Z})^*\to\mathbf{C}$, 它在 a 取值为 1, 在其他取 0, 即得证明. □

5.2. 对偶群

注记 I.2.27. — 如果 G 为群, 那么 $\widehat{G}$ 在线性特征标的乘法 $[\chi_1\chi_2(x)=\chi_1(x)\chi_2(x)$, 其中 $x\in G$, $\chi_1,\chi_2\in\widehat{G}]$ 下是个交换群, 因此我们还可以考虑它的线性表示的群 $\widehat{\widehat{G}}$. 上面的乘法公式证明了, 如果 $x\in G$, 则 $\chi\mapsto\chi(x)$ 是 $\widehat{G}$ 的一个线性特征标; 由此得到一个自然映射 $\iota:G\to\widehat{\widehat{G}}$, 其定义为 $(\iota(x))(\chi)=\chi(x)$. 因为对于 $x,y\in G$ 和所有的 $\chi\in\widehat{G}$ 有

$$(\iota(xy))(\chi)=\chi(xy)=\chi(x)\chi(y)=(\iota(x))(\chi)(\iota(y))(\chi),$$

即 $\iota(xy)=\iota(x)\iota(y)$, 故这个映射是一个群态射.

命题 I.2.28. — 如果 G 是有限的交换群, 则 $\iota:G\to\widehat{\widehat{G}}$ 是一个群同构.

证明 考虑到上面的讨论, 只需再证明 ι 是双射就可以了. 如果 H 是个有限的交换群, 则由推论 I.2.25 有 $|\mathrm{Conj}(H)|=|H|$ 和 $|\mathrm{Irr}(H)|=|\widehat{H}|$, 因此利用推论 I.2.16 便得到 $|H|=|\widehat{H}|$. 对于 G 和 $\widehat{G}$ 用此结果便知 G 和 $\widehat{\widehat{G}}$ 具有相同的基数. 因此只要验证 ι 为单射就足够了. 但在前节的命题 I.2.26 中引进的函数 ϕ_a 的傅里叶分解证明了, 如果对每个 $\chi\in\widehat{G}$ 有 $\chi(a)=\chi(b)$, 则 $\phi_a=\phi_b$, 从而 $a=b$. 得证. □ [249]

习题 I.2.29. — 证明 $\mathbf{Z}/n\mathbf{Z}$ 的对偶群同构于 $\mathbf{Z}/n\mathbf{Z}$(事实上, 同构于 $\boldsymbol{\mu}_n$).

引理 I.2.30. — 设 G 是有限的交换群.

(i) 如果 $x\in G$ 的阶为 a, $y\in G$ 的阶为 b, 而 a 与 b 互素, 则 xy 的阶为 ab.

(ii) 如果 $a,b\in\mathbf{N}-\{0\}$, 且 G 含有阶为 a 和 b 的元, 则它也包含了阶为 $\mathrm{lcm}(a,b)$ 的元.

(iii) 设 N 是 G 中的元的阶的最大者, 则对于所有 $x\in G$ 有 $x^N=1$.

证明 (i) 由于 x,y 交换, 故 $(xy)^n=x^ny^n$, $n\in\mathbf{N}$. 特别地, $(xy)^{ab}=x^{ab}y^{ab}=1$, 因此 xy 的阶整除 ab. 反之, 如果 $(xy)^n=1$, 则 $1=(xy)^{an}=y^{an}$ 以及 $1=(xy)^{bn}=x^{bn}$,

[39]由于 "模" 字的多含义, 有时便直接写为 mod D 的狄利克雷特征标.

从而 an 是 b 的倍数, 而 bn 是 a 的倍数. 但 a 和 b 互素, 这表明 n 是 a 和 b 的倍数, 从而是 ab 的倍数; 换句话说, xy 的阶是 ab 的倍数. 由此得 (i).

(ii) 令 $\mathscr{P}_1$(分别地, $\mathscr{P}_2$) 为使得 $v_p(a)>0$ 和 $v_p(a)\geqslant v_p(b)$ (分别地, $v_p(b)>v_p(a)$) 的素数 p 的集合. 于是 $\mathscr{P}_1$ 与 $\mathscr{P}_2$ 互不相交, 因此 $k=\prod_{p\in\mathscr{P}_1}p^{v_p(a)}$ 和 $\ell=\prod_{p\in\mathscr{P}_2}p^{v_p(b)}$ 互素. 另外, 如果 $v_p(a)\geqslant v_p(b)$, 则有 $v_p(k\ell)=v_P(a)$, 而 $v_p(a)<v_P(b)$, 则有 $v_p(k\ell)=v_p(b)$, 因此 $k\ell=\mathrm{lcm}(a,b)$. 现在设 $x\in G$ 的阶为 a 而 $y\in G$ 的阶为 b. 因为 k 整除 a, 故表明 $x'=x^{a/k}$ 的阶为 k. 同样, $y'=y^{b/\ell}$ 的阶为 ℓ. 那么 (i) 表明 $x'y'$ 的阶为 $k\ell=\mathrm{lcm}(a,b)$. 得到了 (ii).

(iii) 如果 $x\in G$ 是阶为 a 的元, 则由 (ii) 得知 G 包含了一个阶为 $\mathrm{lcm}(a,N)$ 的元. 由于 $\mathrm{lcm}(a,N)\geqslant N$, 那么按 N 的定义知 $\mathrm{lcm}(a,N)=N$, 从而 a 整除 N. 得到 (iii). □

注记 I.2.31. — 情形 S_3 表明引理 I.2.30 的第三个结果当 G 不交换时不成立.

如果 G 是个有限的交换群, 称引理 I.2.30(iii) 中具有所描述的那些性质的 N 为 G 的指数[40].

引理 I.2.32. — 如果 G 为有限的交换群, 则 G 和 $\widehat{G}$ 具有相同的指数.

[250] 证明 如果 H 是个有限的交换群, 以 $N(H)$ 记其指数. 如果 $\chi\in\widehat{H}$, 则对所有的 $x\in G$ 有

$$\chi^{N(H)}(x)=\chi(x)^{N(H)}=\chi(x^{N(H)})=\chi(1)=1,$$

因此 $\chi^{N(H)}=1$. 于是 $\widehat{H}$ 的指数整除 H 的指数. 将此结果用于 $H=G$ 和 $H=\widehat{G}$ 以及 $\widehat{\widehat{G}}\cong G$ 便得到了不等式 $N(G)=N(\widehat{\widehat{G}})\leqslant N(\widehat{G})\leqslant N(G)$. 故得结论. □

5.3. 有限交换群的结构定理

定理 I.2.33. — 如果 G 为有限的交换群, 则存在 $r\in\mathbf{N}$ 和整数 $N_1,\ldots,N_r$, 其中 N_1 是 G 的指数, 而 $N_{i+1}\mid N_i$, $i\leqslant r-1$, 使得 $G\cong\oplus_{i=1}^r\mathbf{Z}/N_i\mathbf{Z}$.

证明 由对 $|G|$ 进行归纳证明. 如果 $|G|=1$, 结论平凡 ($r=0$). 假设 $|G|>1$, 以 $N=N_1$ 记 G 的指数. 于是对于所有的 $\chi\in\widehat{G}$ 和 $x\in G$, $\chi(x)$ 是一个 N 次单位根. 另外, 由于 N 也是 $\widehat{G}$ 的指数 (引理 I.2.32), 故存在阶为 N 的 χ_1, 由于 $\chi(G)$ 是循环群 $\boldsymbol{\mu}_N$ 的子群, 从而是整个的 $\boldsymbol{\mu}_N$. 那么便存在 $x_1\in G$ 使得 $\chi_1(x_1)=e^{2i\pi/N}$. 因为 x_1 的阶整除 N, 由群的指数的定义得到 x_1 的阶为 N, 从而 G 的由 x_1 生成的子群 H_1 同构于 $\mathbf{Z}/N\mathbf{Z}$. 我们将证明 G 是 H_1 和 $G_1=\mathrm{Ker}\chi_1$ 的直和. 如果得证, 则因为一个子群的指数显然整除群的指数, 于是对 G_1 应用归纳假定就可得到结论. 为此, 首先我们发现 χ_1 诱导了 H_1 到 $\boldsymbol{\mu}_N$ 的同构: 它是满的同时具有相同的基数 N; 以 $\alpha:\boldsymbol{\mu}_N\to H_1$ 记其逆. 如果 $x\in G$, 则 $a=\alpha(\chi_1(x))\in H_1$, 并且 $b=a^{-1}x$ 满足 $\chi_1(b)=\chi_1(a)^{-1}\chi_1(x)=1$, 从而 $b\in G_1$. 于是可以将 G 的所有元 x 写为形

[40]这里用的相当于英文中的 "exponent", 不同于群指数 "index", 尽管中文都翻译作 "指数".

式 $x = ab$, $a \in H_1$, $b \in G_1$. 最后因为 χ_1 在 H_1 上为单的, 故 $H_1 \cap G_1 = \{1\}$. 这证明了 $G = H_1 \oplus G_1$, 得到结论. □

习题 I.2.34. — 设 G 为有限的交换群. 证明 $\widehat{G}$ 同构于 G.

6. 有限群的特征标表

设 G 为有限群, 而 $c = |\mathrm{Conj}(G)|$. G 的特征标表是一个 $c \times c$ 的表格, 其系数是不可约特征标在 G 的共轭类上的值, 在对应于特征标 χ 的列和对应共轭类 C 的行的相交处的系数为 $\chi(C)$. 这是群 G 的某种名片.

注记 I.2.35. — 以 T_G 记由特征标表定义的 $c \times c$ 矩阵. 也以 K 记那样的对角矩阵, 它的对应于共轭类 C 的行上的对角系数为 $\frac{|C|}{|G|}$. 于是特征标的正交关系可以紧凑地表达成 $T_G^* K T_G = 1$. 由此得到 $K = (T_G^*)^{-1} T_G^{-1}$ 和 $K^{-1} = T_G T_G^*$. 特别地, T_G 的行构成了一个正交族, 这使我们在只知道一部分信息时可以填满这个特征标表. [251]

举例说, 群 $\{\pm 1\}$ 有两个共轭类 1 和 -1, 即两个不可约特征标 $\mathbf{1}$ 和 χ(因为 $\{\pm 1\}$ 交换, 具维数 1); 容易建立它的特征标表, 见图 1.

	$\mathbf{1}$	χ
1	1	1
-1	1	-1

图 1. 群 $\{\pm 1\}$ 的特征标表

群 $\{\pm 1\}$ 的例子对于给出如何构建一个群的特征标表的方法来说有点太简单了. 下面要处理的例子 A_4 则要丰富得多. 读者可以在习题中找到建立小的群的特征标表的其他技术. 附录 C 和问题 H.2, H.3 和 H.4 包含了一些更精妙的例子. 一般理论的简洁和威力与特别情形的手工处理间形成了强烈的对照.

回忆一下: A_4 是 S_4 的符号差为 1 的置换子群. 因为 S_4 有 24 个元, 故 $|A_4| = 12$, 并且 A_4 的元为:

- 中性元 id.
- 两个对换的乘积中的三个: $s_2 = (12)(34)$, $s_3 = (13)(24)$, $s_4 = (14)(23)$, 它们的阶均为 2.
- 八个 3-循环:(123), (234), (341), (412) 和 (132), (243), (314), (421), 它们的阶均为 3.

我们打算构建 A_4 的特征标表. 有多种可以达到目的的途径. 最系统的方法是先决定 A_4 的共轭类, 再构造出 A_4 的所有不可约表示, 然后计算它们的特征标在共轭类上

的值. 这是我们首先要研究的[7]; 然后我们用书中的一些定理去证明上述方法中有些是可以简化的.

(a) 设 t 为 3-循环 (123). 我们有 $t^2 = (132)$, 而因为 t 的阶等于 3, 故 A_4 的由 t 生成的子群 $T = \{1, t, t^2\}$ 的阶等于 3.

(b) $H = \{\mathrm{id}, s_2, s_3, s_4\}$ 是 A_4 的一个正规的交换子群.

[252] 「 这些可以经过有点麻烦的计算得到证明. 还需注意到, A_4 一个 2-西罗群的基数等于 4, 而由于 H 的基数为 4 并包含 A_4 中其阶整除 4 的元, 这证明只有单独的一个 2-西罗群 (因为共轭将一个 2-西罗变换为一个 2-西罗, 故它是正规的), 它就是 H. 另外, H 的所有元的阶都整除 2, 而具有这个性质的群由于 $(xy)^2 = 1 = x^2y^2$ 表明 $xy = yx$ 是交换的. 」

(c) A_4 的每个元都可以以唯一的方式写成形式 $t^a h$, 其中 $a \in \{0, 1, 2\}$ 而 $h \in H$.

「 A_4 的子群 T 和 H 的交为 $\{\mathrm{id}\}$. 由此得到 $(c, h) \mapsto ch$ 是 $T \times H$ 到 A_4 的一个单射; 实际上, 如果 $c_1h_1 = c_2h_2$, 则 $c_2^{-1}c_1 = h_2h_1^{-1}$, 而由于 $c_2^{-1}c_1 \in T$ 和 $h_2h_1^{-1} \in H$, 故 $c_1 = c_2$, $h_2 = h_1$. 因为 $T \times H$ 与 A_4 的基数相同, 一个单射便是一个双射. 得证. 」

(d) t 和 t^2 不与 $H - \{\mathrm{id}\}$ 中的任何元交换.

「 这可以通过稍微难一点的计算来证明. 我们也可以注意到, 如果 t 和 $s \in H - \{\mathrm{id}\}$ 交换, 那么 A_4 的由 t 和 s 生成的子群 G 为交换群, 并且由于有 s 和 t 生成的子群 $\{\mathrm{id}, s\}$ 和 T 构成 G 直和, 故而 G 同构于 $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/3\mathbf{Z}) \cong \mathbf{Z}/6\mathbf{Z}$. 但因为 A_4 不包含阶为 6 的元, 故这是不可能的. 对于任意的 3-循环, 特别对于 t^2 也可进行同样的推理. 」

(e) A_4 的共轭类是 $B_1 = \{\mathrm{id}\}$, $B_2 = H - \{\mathrm{id}\}$, $B_3 = tH$ 和 $B_4 = t^2H$.

「 通过十分繁复的计算可以得出结论:

- 由于在所有的群中中性元的等价类只有一个元, 从而 $B_1 \in \mathrm{Conj}(A_4)$.
- 如果 $s \in B_2$, 而对于 $a \in \{0, 1, 2\}$ 和 $h \in H$, $t^a h$ 与 s 交换, 则有 $t^a hs = st^a h$, 从而 $t^a hsh = st^a h^2$, 并且由于 H 是个交换群, $h^2 = \mathrm{id}$, 故得到 $t^a s = st^a$, 这意味着 $a = 0$. 于是 H 便是 s 的中心化子, 那么 s 的共轭类的基数等于 $\frac{|A_4|}{|H|} = 3$. 因为一个 s 的共轭元记阶为 2, 这个类必定包含在 B_2 中, 由于基数的原因它们相等.
- 最后, t 和 t^2 的中心化子为 T (如果 $t^a ht = tt^a h$, 则有 $ht = th$, 从而 $h = \mathrm{id}$), 这使得 t 的共轭类的基数等于 $\frac{|A_4|}{|T|} = 4$. 然而因为 H 为正规的, 我们有 $t^{a-1}ht^{1-a} \in H$ 和 $t^a h^{-1} t^{-a} \in H$, 故 $(t^a h)t(t^a h)^{-1} = t^a hth^{-1}t^{-a} = t(t^{a-1}ht^{1-a})(t^a h^{-1} t^{-a} \in tH$. 因此 t 的共轭类包含在 B_3 中, 并由于基数的原因与它相等. 同样, t^2 的共轭类是 B_4.

证完. 」

(f) 设 $\rho = e^{\frac{2i\pi}{3}}$ 是个 3 次单位元根. 如果 $i \in \{0, 1, 2\}$, 定义 $\eta^i : A_4 \to \boldsymbol{\mu}_3$

[7]我们并没有寻求最简短的解法; 相反, 我们力图尽多地使用有限群理论的基本技术. 能够在利用已知 S_4 的共轭类情形下 (小词典的 3.4 小节) 进行得最迅捷.

为 $\eta^i(t^ah)=\rho^{ia}$, $a\in\{0,1,2\}$, $h\in H$. 于是 $\eta^0=1$, 而 η 和 η^2 为 A_4 的不同的线性特征标.

「 如果 $a,b\in\{0,1,2\}$, 而 $h,g\in H$, 则 $t^aht^bg=t^{a+b}(t^{-b}ht^b)g$, 并由于 H 正规, 故有 $t^{-b}ht^b\in H$, 从而 $(t^{-b}ht^b)g\in H$, 以及 $\eta^i(t^aht^bg)=\rho^{i(a+b)}=\rho^{ia}\rho^{ib}=\eta^i(t^ah)\eta^i(t^bg)$. 」

(g) 设 V 是与 A_4 的自然作用于 $\{1,2,3,4\}$ 的相伴置换表示. 我们已知这个表示是具有 A_4 作用的 $\mathbf{C}^4$, 其定义是在典范基 $e_1,\ldots,e_4$ 上有 $g(e_i)=e_{g(i)}$. 由方程 $x_1+\cdots+x_4=0$ 定义的超平面 W 在 A_4 下稳定, 并且得到的表示是不可约的, 给出其特征标如下: $\chi_W(\mathrm{id})=3$, 而当 $g\in H-\{\mathrm{id}\}$ 时 $\chi_W(g)=-1$; 当 $g\notin H$ 时 $\chi_W(g)=0$. [253]

「 表示 V 可分解为 $V'\oplus W$ 的形式, 其中 V' 是由 $e_1+\cdots+e_4$ 生成的直线 (因为 $e_1+\cdots+e_4$ 在 A_4 下稳定, 故同构于 $\mathbf{1}$). 由于 V 是置换表示, $\chi_V(g)$ 是 g 作用在 $\{1,2,3,4\}$ 上的不动点的个数. 因此 $\chi_V(\mathrm{id})=4$, 而当 $g\in H-\{\mathrm{id}\}$ 时 $\chi_V(g)=0$, 当 $g\notin H$ 时 $\chi_V(g)=1$. 因为 $\chi_V=\chi_{V'}+\chi_W$, 又因为 $V'\cong\mathbf{1}$ 从而对所有的 $g\in G$ 有 $\chi_{V'}(g)=1$, 故由此得到 W 的特征标. 因此 $\chi_W(\mathrm{id})=3$, 而当 $g\in H-\{\mathrm{id}\}$ 时 $\chi_W(g)=-1$; 当 $g\notin H$ 时 $\chi_W(g)=0$.

还需验证 W 是不可约的. 首先看到, 如果 $g\in A_4$, 且 $v=(x_1,\ldots,x_4)\in\mathbf{C}^4$, 则 $g\cdot v=x_1e_{g(1)}+\cdots+x_4e_{g(4)}=(x_{g^{-1}(1)},\ldots,x_{g^{-1}(4)})$. 现在假设 $v\in W-\{0\}$, 而 W' 是由 $g\cdot v$, $g\in A_4$ 生成的 W 的子空间 (要证明对于任意的 v 有 $W'=W$). 因此存在 $i\neq j$ 使得 $x_i\neq x_j$, 不失一般性, 不妨设 $x_1\neq x_2$. v 在 3-循环 $t=(123)$ 下的像因而是 (x_3,x_1,x_2,x_4); 由此知道, 包含了 $t\cdot v$ 和 v 的 W' 也包含了 $w=t\cdot v-v=(x_3-x_1,x_1-x_2,x_2-x_3,0)$ (因此出现了一个 0). 子空间 W' 也包含了 $w+g\cdot w$, $g=(13)(24)$, 并且由于 $w+g\cdot w=(x_1-x_2)(e_2+e_4-e_1-e_3)$ 和 $x_1-x_2\neq 0$, 因此它包含了向量 $f_1=e_1-e_2+e_3-e_4$. 它也包含了这个向量在 3-循环 (243) 和 (234) 作用下的像 $f_2=e_1+e_2-e_3-e_4$ 和 $f_3=e_1-e_2-e_3+e_4$; 因为 f_1,f_2,f_3 构成了 W 的一组基, 故有 $W'=W$, 断言得证. 」

(h) A_4 的特征标表由图 2 给出.

	$\mathbf{1}$	η	η^2	χ_W
B_1	1	1	1	3
B_2	1	1	1	-1
B_3	1	ρ	ρ^2	0
B_4	1	ρ^2	ρ	0

图 2. A_4 的特征标表

事实上, A_4 有 4 个共轭类, 它也有在同构意义下不同的 4 个不可约表示, 它们

是 3 个线性特征标 $1,\eta,\eta^2$ 和 3 维表示 W. 这些表示的特征标的值已在上面算出了; 也就是表中的值. 故得结论.

「 • 第一个简化. 利用推论 I.2.21 证明 W 的不可约性: 我们有 $\langle\chi_W,\chi_W\rangle = \frac{1}{12}(3^2+3\cdot(-1)^2+8\cdot 0)=1$, 这表明 W 不可约.

• 第二个简化. 想象我们已构造出了表示 $1,\eta,\eta^2$ 和 W 的特征标在 B_1,B_2,B_3 和 B_4 上取表中的值, 但并不知道哪些是 A_4 的共轭类. 那么可以由此推导出这些共轭类恰好是 B_1,B_2,B_3 和 B_4, 这便可以省掉上面的 (d) 和 (e) 了. 事实上, 由于 $1^2+1^2+1^2+3^2=12$, 故伯恩赛德公式 (推论 I.2.23 的 (ii)) 表明 $1,\eta,\eta^2$ 和 χ_W 是 $\mathrm{Irr}(A_4)$ 的元, 因而 (推论 I.2.16) A_4 有 4 个共轭类. 但注意, 如果 $i\neq j$, 则存 [254] 在 $\chi\in\mathrm{Irr}(A_4)$ 在 B_i 和 B_j 上取不同的值. 由于 $\mathrm{Irr}(A_4)$ 的元在共轭类上为常值, 因此知, 如果 $C\in\mathrm{Conj}(A_4)$, 则存在 $i(C)\in\{1,2,3,4\}$ 使得 $C\subset B_{i(C)}$. 这些元 C 形成了 A_4 的一个分拆, 映射 $C\mapsto i(C)$ 从而为满射, 并且因为这两个集合的元素个数相同, 故为双射; 另外, 我们有 $B_{i(C)}=C$, 否则 $B_{i(C)}-C$ 将不在共轭类的并集中了. 总起来, A_4 的共轭类就是这些 B_i.

• 第三个简化. 假定已经构造了 W. 于是伯恩赛德公式 (推论 I.2.23 的 (ii)) 给了我们恒等式 $12=|A_4|=9+\sum_{W'\in\mathrm{Irr}(A_4)-\{W\}}(\dim W')^2$, 因为 3 只有一种写成平方和的方法, 故推出 A_4 有三个线性特征标. 换而言之, 群 $\widehat{A}_4$ (参看习题 I.1.10) 的基数为 3, 从而同构于 $\mathbf{Z}/3\mathbf{Z}$; 特别地, 它是循环的, 并且如果 η 是一个生成元, $\widehat{A}_4$ 的元素是 η,η^2 和等于 η^3 的平凡特征标. 由于 η 的阶为 3, 故它取值在 3 次单位根的群 $\boldsymbol{\mu}_3$ 中; 而它的像是 $\boldsymbol{\mu}_3$ 的非 $\{1\}$ 的子群, 故是整个 $\boldsymbol{\mu}_3$. 特别 η 的像的基数为 3, 因而其核的基数为 $|A_4|/3=4$. 另外, 因为 $\boldsymbol{\mu}_3$ 的阶数整除 2 的唯一元是 1, 故 $H\subset\mathrm{Ker}\chi$. 由此推出 $\mathrm{Ker}\chi=H$, 重新证明了 (b). 最后, 在 $\eta(t)\neq 1$ 下, 因为 $t\notin H$, 故有 $\eta(t)=\rho$ 或者 $\eta(t)=\rho^2$; 如有必要可将 η 换作 η^2, $\eta(t)=\rho$. 于是当 $g\in H=B_1\cup B_2$ 时有 $\eta(g)=1$, 而当 $g\in B_3=tH$ 时有 $\eta(g)=\rho$, 以及 $g\in B_4=t^2H$ 时有 $\eta(g)=\rho^2$. 应用第二个简化便可以完成 A_4 的特征标表而无需利用关于 A_4 结构的 (a)—(e) 也无需用 (f).

• 第四个简化. 这一次我们假设已经构造了 η, 而且只利用了 (a)—(c) 和 (f) 但没有用 (d), (e) 和 (g). 伯恩赛德公式已经表明对于线性特征标 1, η, η^2 的不可约特征标有四种可能性:

— 一个 3 次的唯一的特征标 χ_W,

— 两个 2 次的特征标和一个 1 次的特征标, 或者一个 2 次的和五个 1 次的,

— 九个 1 次的特征标.

如果是第一种情形, 因为 $1+\eta+\eta^2+3\chi_W$ 是正则表示的特征标, 故让我们可以计算 χ_W, 于是用第二个简化便可完成这张表. 因此只要消去其他的可能性就可以了.

⋆ 最后一种情形表明 $|\mathrm{Irr}(A_4)|=12$, 这又表明 A_4 有 12 个共轭类 (推论 I.2.16), 因而它们都是单个的, 从而 A_4 成为交换的, 这不可能.

⋆ 如果 A_4 至少有一个 2 维的不可约表示 V, 于是 $\chi_V, \chi_V\eta, \chi_V\eta^2$ 都是 2 次的不可约特征标 (参看 2.1 节), 并且由于最多只有两个这样的特征标, 故存在 $\eta_1 \neq \eta_2 \in \{1, \eta, \eta^2\}$ 使得 $\chi_V\eta_1 = \chi_V\eta_2$. 然而条件 $\eta_1 \neq \eta_2$ 表明 $\eta_1(t) \neq \eta_2(t)$, 而关系式 $\chi_V\eta_1 = \chi_V\eta_2$ 导致了 $\chi_V(t) = 0$. 由于 t 的阶为 3, 这使得 ρ_V 的两个特征值都是 3 次单位根, 3 次单位根的任两个的和从不为零, 故这是不可能的. 因此 2 维的不可约表示是不存在的. 结论得证. ⌟

I.3. 构造表示

1. 限制和提升

如果 H 是 G 的一个子群, V 是 G 的表示, 我们可以不管 $g \in G - H$ 上的作用而考虑 V 在 H 上的限制 $\mathrm{Res}_G^H V$. 于是 $\rho_{\mathrm{Res}_G^H V} : H \to \mathrm{GL}(V)$ 是 $\rho_V : G \to \mathrm{GL}(V)$ 在 H 上的限制, 而 $\chi_{\mathrm{Res}_G^H V}(h) = \chi_V(h)$, 其中任意 $h \in H$.

如果 $\varphi : G \to H$ 是一个群态射, 且 V 是 H 的一个表示, 则 V 可以看成是 G 的一个表示, 其中 $g \in G$ 的作用由 $\varphi(g) \in H$ 给出; 这样得到的 G 的表示是从 V 到 G 的提升 $\mathrm{Inf}_H^G V$. 于是 $\rho_{\mathrm{Inf}_H^G V} : G \to \mathrm{GL}(V)$ 等于复合 $\rho_H \circ \varphi$, 从而对所有的 $g \in G$ 有 $\chi_{\mathrm{Inf}_H^G V}(g) = \chi_V(\varphi(g))$. 如果 χ 是 H 的一个特征标, 于是由前面的结果得到 $\chi \circ \varphi$ 是 G 的一个特征标; 称其为从 χ 到 G 的提升. [255]

注记 I.3.1. — 设 $\varphi : G \to H$ 为满射.

(i) V 的一个子空间在 G 下稳定当且仅当它在 H 下稳定, 这证明了 $\mathrm{Inf}_H^G V$ 不可约当且仅当 V 不可约, 也证明了 $\chi \mapsto \chi \circ \varphi$ 诱导了一个从 $\mathrm{Irr}(H)$ 到 $\mathrm{Irr}(G)$ 的单射.

(ii) 如果 N 是 φ 的核, G 的一个表示 V 由 H 的一个表示的提升得到当且仅当 N 在 V 上的作用为平凡的; 事实上, 如果 $V = \mathrm{Inf}_H^G W$, 那么 $g \in N$ 在 W 上的作用由 $\varphi(g) = 1$ 给出, 从而 N 平凡地作用于 V; 反之, 如果 V 是 G 的一个表示, 在其上 N 的作用为平凡的, 则 V 是由 $h \cdot v$, $h \in H$, $v \in V$ 定义的表示提升, 其定义为 $v \mapsto \tilde{h} \cdot v$, 其中 $\tilde{h} \in H$ 满足 $\varphi(\tilde{h}) = h$: 它不依赖于 $\tilde{h}$ 的选取, 否则由于 N 的作用平凡, 如果 $\varphi(\tilde{h}) = \varphi(\tilde{h}')$, 则表明存在 $n \in N$ 使得 $\tilde{h}' = \tilde{h}n$, 因而 $\tilde{h}' \cdot v = \tilde{h} \cdot (n \cdot v) = \tilde{h} \cdot v$.

习题 I.3.2. — 设 G 为有限群, $\varphi : G \to H$ 是一个满的群态射, 其核为 N. 证明 $\chi \in \mathrm{Irr}(G)$ 是 H 的一个特征标的提升当且仅当对所有的 $g \in N$ 有 $\chi(g) = \chi(1)$.

2. 表示的张量构造

2.1. 有限维向量空间的张量积

设 V_1, V_2 为两个有限维的向量空间, 并设 $(e_1, \ldots, e_n)$ 为 V_1 的一组基, 而 $(f_1, \ldots, f_m)$ 为 V_2 的一组基. 令 $V_1 \otimes V_2$ 为 V_1 和 V_2 的张量积: 这是一个具有基 $e_i \otimes f_j$, $1 \leqslant i \leqslant$

n, $1 \leqslant j \leqslant m$ 的向量空间[8]. 如果 $x = \sum_{i=1}^{n} \lambda_i e_i \in V_1$ 和 $y = \sum_{j=1}^{m} \mu_j f_j \in V_2$, 则以 $x \otimes y$ 记 $V_1 \otimes V_2$ 中由公式

$$x \otimes y = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_i \mu_j e_i \otimes f_j$$

定义的元. 张量积 $V_1 \otimes V_2$ 一般来说是一个新的对象, 但它可以以更显式的方式写出来.

习题 I.3.3. — (i) 如果 X 是个有限集, 以 $\mathbf{C}^X$ 记函数 $\pi : X \to \mathbf{C}$ 的集合. 这是一个以集合 ϕ_x, $x \in X$ 为基的向量空间, 其中当 $y = x$ 时 $\phi_x(y) = 1$, 而当 $y \neq x$ 时 $\phi_x(y) = 0$. 容易证明, 如果 I 和 J 是两个有限集, 则 $\phi_i \otimes \phi_j \to \phi_{(i,j)}$, $i \in I$, $j \in J$ 诱导了从 $\mathbf{C}^I \times \mathbf{C}^J$ 到 $\mathbf{C}^{I \times J}$ 的同构.

[256] (ii) 如果 V_1, V_2 是两个向量空间, 而 V_1^*, V_2^* 是它们的对偶 (V_i^* 是 V_i 上的线性形式的空间), 则 $V_1^* \otimes V_2^*$ 是 $V_1 \times V_2$ 上的双线性形式的空间. 如果 $\lambda_1 \in V_1^*$ 而 $\lambda_2 \in V_2^*$, 则 $\lambda_1 \otimes \lambda_2$ 是双线性形式 $(x, y) \mapsto \lambda_1(x)\lambda_2(y)$.

习题 I.3.4. — 证明 $V_1^* \otimes V_2 = \mathrm{Hom}(V_1, V_2)$.

由构造知, $(x, y) \mapsto x \otimes y$ 是从 $V_1 \times V_2$ 到 $V_1 \otimes V_2$ 的双线性映射. 下面的引理证明 $V_1 \otimes V_2$ 对于在 $V_1 \times V_2$ 的双线性映射是万有的.

引理 I.3.5. — *如果 W 是个向量空间, 且 $u : V_1 \times V_2 \to W$ 为双线性映射, 则存在唯一的线性映射 $\tilde{u} : V_1 \otimes V_2 \to W$ 使得对于任意的 $x \in V_1$ 和 $y \in V_2$ 有 $\tilde{u}(x \otimes y) = u(x, y)$.*

证明　在基的元 $e_i \otimes f_j$ 上令 $\tilde{u}(e_i \otimes f_j) = u(e_i, f_j)$ 以定义 $\tilde{u}$. 直接的计算证明, u 的双线性性等价于 $\tilde{u}(x \times y) = u(x, y)$, 其中 $x \in V_1$, $y \in V_2$ 任意. 从而得到结论[9]. □

现在, 如果 $u_1 \in \mathrm{End}(V_1)$ 而 $u_2 \in \mathrm{End}(V_2)$, 则 $(x, y) \mapsto u_1(x) \otimes u_2(x)$ 是 $V_1 \times V_2$ 到 $V_1 \otimes V_2$ 的双线性映射. 根据引理 I.3.5, 存在 $u_1 \otimes u_2 \in \mathrm{End}(V_1 \otimes V_2)$ 使得对任意

---

[8] 我们也可以记 $V_1 \otimes V_2$ 的基为 $g_{i,j}$, 但下文中更常提及的是记号 $e_i \otimes e_j$.

[9] 将 $V_1 \otimes V_2$ 考虑为一个泛问题的解, 从而让我们可以证明其构造与 V_1 和 V_2 的基的选取无关. 事实上, 如果 X 是一个具有双线性映射 $B : V_1 \times V_2 \to X$ 的向量空间, 使得对每个双线性映射 $u : V_1 \times V_2 \to W$, 存在唯一的线性映射 $\tilde{u} : X \to W$ 满足对任意的 $x \in V_1$ 和 yV_2 有 $\tilde{u}(B(x, y)) = u(x, y)$, 于是对于每个 $(x, y) \in V_1 \times V_2$ 存在唯一的线性映射 $f : V_1 \otimes V_2 \to X$ 满足 $f(x \otimes y) = B(x, y)$, 以及唯一的线性映射 $g : X \to V_1 \otimes V_2$ 满足对于每个 $(x, y) \in V_1 \times V_2$ 有 $g(B(x, y)) = x \otimes y$. 由于恒等映射是 $V_1 \otimes V_2$(分别地, X) 自身的满足 $h(x \otimes y) = x \times y$ (分别地, $h(B(x, y)) = B(x, y)$) 的唯一的线性映射 h, 其中 $(x, y) \in V_1 \times V_2$ 任意, 故有 $f \circ g = \mathrm{id}_X$ 和 $g \circ f = \mathrm{id}_{V_1 \otimes V_2}$, 这证明了 X 和 $V_1 \otimes V_2$ 同构, 并在差一个 $V_1 \times V_2$ 上的双线性形式的同构下唯一确定. 一个不用选取基的一般性构造是: 将由每个 $(x, y) \in V_1 \times V_2$ 为基的向量空间对关系 $e_{x, y_1 + y_2} = e_{x, y_1} + e_{x, y_2}$, $e_{x_1 + x_2, y} = e_{x_1, y} + e_{x_2, y}$ 和 $e_{\lambda x, y} = e_{x, \lambda y} = \lambda e_{x, y}$ 取商. 则 $x \otimes y$ 是 $e_{x, y}$ 在此商空间中的像 (参看小词典的 10.5.2 节, 那里有相似的构造). 书中的构造虽不太典范但却更具体 …… 一般型的构造的好处还在于可以在无限维情形中进行, 在那里基族并非常常可以明显表示出的.

的 $x \in V_1$ 和 $y \in V_2$ 有 $(u_1 \otimes u_2)(x \otimes y) = u_1(x) \otimes u_2(y)$. 如果 $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathbf{M}_n(\mathbf{C})$ 是 u_1 的矩阵, 而 $B = (b_{i',j'})_{i \leqslant i',j' \leqslant m} \in \mathbf{M}_m(\mathbf{C})$ 是 u_2 的矩阵, 则 $u_1 \otimes u_2$ 在基 $e_i \otimes f_{i'} = g_{(i-1)m+i'}$ 下的矩阵 $A \otimes B \in M_{nm}(\mathbf{C})$ 是 $c_{(i-1)m+i',(j-1)m+j'}$, $1 \leqslant i,j \leqslant n$, $1 \leqslant i',j' \leqslant m$ 的矩阵, 其中 $c_{(i-1)m+i',(j-1)m+j'} = a_{i,j}b_{i'j'}$. 特别有

$$\mathrm{Tr}(u_1 \otimes u_2) = \sum_{1 \leqslant k \leqslant nm} c_{k,k} = \sum_{i=1}^{n}\sum_{i'=1}^{m} a_{i,i}b_{i',i'} = (\sum_{i=1}^{n} a_{i,i})(\sum_{i'=1}^{m} b_{i'.i'}) = \mathrm{Tr}(u_1)\mathrm{Tr}(u_2).$$

最后, 由引理 I.3.5 得到, 如果 $u_1', u_1'' \in \mathrm{End}(V_1)$, 而 $u_2', u_2'' \in \mathrm{End}(V_2)$, 则 [257]

$$(u_1' \circ u_1'') \otimes (u_2' \circ u_2'') = (u_1' \otimes u_2') \circ (u_1'' \otimes u_2'').$$

(只要比较 $x \otimes y$ 在两端的像即可.)

2.2. 表示的张量积

设 G 是个有限群, 而 V_1, V_2 是 G 的两个表示. 按照前所述, 如果定义 G 在 $V_1 \otimes V_2$ 的作用为 $g \cdot (x \otimes y) = (g \cdot x) \otimes (g \cdot y)$, 则得到 G 的一个表示. 上面关于 $u_1 \otimes u_2$ 的迹的公式表明

$$\chi_{V_1 \otimes V_2}(g) = \chi_1(g)\chi_2(g).$$

如果 V_2 为一维的, 则又回到了一个线性特征标对表示的扭变 (§I.1 的 2.1 节).

注记 I.3.6. — (i) 如果 G_1 和 G_2 是两个有限群, 其 V_1 和 V_2 分别是 G_1 和 G_2 的表示, 我们可以以相同的方式定义 $G_1 \times G_2$ 的一个表示 $V_1 \boxtimes V_2$, 其定义为 $g = (g_1, g_2) \in G_1 \times G_2$ 以 $g \cdot (x \otimes y) = (g_1 \cdot x) \otimes (g_2 \cdot y)$ 作用到 $V_1 \otimes V_2$ 上.

(ii) 如果 $G_1 = G_2 = G$, 前面定义的 G 的表示 $V_1 \otimes V_2$ 是 $G \times G$ 的表示 $V_1 \boxtimes V_2$ 在 G 上的限制, 其中的 G 看作 $G \times G$ 中 (g, g) 的集合 (为了区分不将 $V_1 \boxtimes V_2$ 记为 $V_1 \otimes V_2$).

习题 I.3.7. — 证明 $R^+(G)$ 在乘积下稳定, 而 $R_{\mathbf{Z}}(G)$ 是一个环.

习题 I.3.8. — 用取 g 的特征向量的方法再次给出公式 $\chi_{V_1 \otimes V_2}(g) = \chi_1(g)\chi_2(g)$.

2.3. 表示的对称方和外积方

如果 V 是有限群 G 的一个表示, 则表示 $V \otimes V$ 不是不可约的. 事实上, 对称张量 (即形如 $xy = \frac{1}{2}(x \otimes y + y \otimes x)$, $x, y \in V$ 的向量, 因而对于 $x, y \in V$ 有 $xy = yx$) 和交错张量 (即 $x \wedge y = x \otimes y - y \otimes x$, 因而 $x \wedge y = -y \wedge x$, 其中 $x, y \in V$) 在 G 的作用下稳定; 所以在它们生成的 $V \otimes V$ 的子空间也稳定.

以 $\mathrm{Sym}^2 V$ 记 V 的这个对称方; 它是 $V \otimes V$ 的由对称张量生成的子空间. 如果 V 的维数为 d, 基为 $(e_1, \ldots, e_d)$, 则 $\mathrm{Sym}^2(V)$ 是 $\frac{d(d+1)}{2}$ 维的空间, 它的基由 $e_ie_j, 1 \leqslant i \leqslant j \leqslant d$ 构成.

以 $\wedge^2 V$ 记 V 的外积方; 这是 $V \otimes V$ 的由交错张量生成的子空间. 它是一个 $\frac{d(d-1)}{2}$ 维的空间, 它的基由 $e_i \wedge e_j$, $1 \leqslant i < j \leqslant d$ 构成.

另外, $V\otimes V=\mathrm{Sym}^2V\oplus\wedge^2V$(分解为 $V\otimes V$ 的对称算子 s 的特征空间的和, 这里的 s 是由 $V\times V\to V\otimes V:(x,y)\mapsto y\otimes x$ 的线性化得到的; 对于任意 $x,y\in V$ 我们有 $s(x\otimes y)=(y\otimes x)$).

[258] **例题 I.3.9.** — 如果 V^* 是 V 的对偶, 则 Sym^2V^* 是 V 上的对称双线性形式的空间, 而 $\wedge^2V^*$ 则是交错双线性形式的空间.

命题 I.3.10. — *如果 V 是 G 的一个表示而 $g\in G$, 则*

$$\chi_{\mathrm{Sym}^2V}(g)=\frac{1}{2}(\chi_V(g)^2+\chi_V(g^2)),\ \text{以及}\quad \chi_{\wedge^2V}(g)=\frac{1}{2}(\chi_V(g)^2-\chi_V(g^2)).$$

证明　选取由 g 的特征向量构成的一组基 $(e_1,\ldots,e_d)$. 于是有 $g\cdot e_i=\lambda_ie_i$, $g^2\cdot e_i=\lambda_i^2e_i$, 而 $g\cdot e_ie_j=\lambda_i\lambda_je_ie_j$, $g\cdot e_i\wedge e_j=\lambda_i\lambda_je_i\wedge e_j$. 由此得到

$$\chi_{\mathrm{Sym}^2V}(g)=\sum_{i\leqslant j}\lambda_i\lambda_j\ \text{和}\quad \chi_{\wedge^2V}(g)=\sum_{i<j}\lambda_i\lambda_j,$$

又因为

$$\chi_V(g^2)=\sum_i\lambda_i^2,\quad \chi_V(g)^2=(\sum_i\lambda_i)^2=\sum_i\lambda_i^2+2\sum_{i<j}\lambda_i\lambda_i,$$

故得结论. □

注记 I.3.11. — 我们对两份 G 的表示 V 的以上做法可以推广到 V 的 n 份的情形. 以 $\otimes^nV$ 代表 n 份 V 的张量积 (显然的定义). S_n 代表 $\{1,\ldots,n\}$ 的置换群, 而 $\mathrm{sign}:S_n\to\{\pm1\}$ 是符号映射. 一个对称张量是形如

$$x_1\cdot\cdots\cdot x_n=\frac{1}{n!}\sum_{\sigma\in S_n}x_{\sigma(1)}\otimes\cdots\otimes x_{\sigma(n)}$$

的张量, 而一个交错张量是形如

$$x_1\wedge\cdots\wedge x_n=\sum_{\sigma\in S_n}\mathrm{sign}(\sigma)x_{\sigma(1)}\wedge\cdots\wedge x_{\sigma(n)}$$

的张量. V 的 n 次对称幂 Sym^nV 是 $\otimes^nV$ 中由对称张量生成的空间, 而 V 的 n 次外幂 $\wedge^nV$ 则是 $\otimes^nV$ 中由这些交错张量生成的空间. 于是 Sym^nV 和 $\wedge^nV$ 的维数分别为 $\binom{d+n-1}{n}$ 和 $\binom{d}{n}$. (当 $n\geqslant3$ 时, $\mathrm{Sym}^nV\oplus\wedge^nV$ 是 $\otimes^nV$ 的真子空间.)

特别地, 当 $n>d$ 时 $\wedge^nV=0$, 而 $\wedge^dV$ 的维数为 1; 常记这个表示为 $\det V$, g 在 $\det V$ 上的作用是乘以 $\det\rho_V(g)$. (见 6.3 节和小词典中习题 6.1 的类似构造.)

3. 诱导表示

3.1. 诱导表示的特征标

设 H 是 G 的子群, V 是 H 的一个表示. 定义向量空间 Ind_H^GV 为

$$\mathrm{Ind}_H^GV=\{\varphi:G\to V,\varphi(hx)=h\cdot\varphi(x),\forall\,h\in H,\forall\,x\in G\}.$$

设 $S \subset G$ 是 $H \setminus G$ 的一个代表元族. 如果 $x \in G$, 则存在唯一的 $h_x \in H$ 使得 $h_x^{-1}x \in S$. 这让我们建立了从 $\mathrm{Ind}_H^G V$ 到 V^S 的一个同构, 它将 φ 映到 $(\varphi(s))_{s\in S}$, 其中 V^S 是 S 到 V 中的映射的集合: 这个双射的逆将 $(v_s)_{s\in S} \in V^s$ 映到映射 $\varphi : G \to V$, 其定义为 $\varphi(x) = h_x \cdot v_{h_x^{-1}x}$. 要验证 φ 确实是 $\mathrm{Ind}_H^G V$ 中的元, 只要注意 [259] 到当 $h \in H$ 时有 $h_{hx} = hh_x$, 从而

$$\varphi(hx) = hh_x \cdot v_{(hh_x)^{-1}h_x} = hh_x \cdot v_{h_x^{-1}x} = h \cdot (h_x \cdot v_{h_x^{-1}x}) = h \cdot \varphi(x).$$

在 $\mathrm{Ind}_H^G V$ 上定义 G 的作用 $g \cdot \varphi$ 为函数 $x \mapsto \varphi(xg)$. 如果 $h \in H$, 则有

$$(g \cdot \varphi)(hx) = \varphi(hxg) = h \cdot \varphi(xg) = h \cdot ((g \cdot \varphi)(x)),$$

这证明了 $g \cdot \varphi$ 是 $\mathrm{Ind}_H^G V$ 中的元. 另外, 如果 $g_1, g_2 \in G$, 则

$$(g_1 \cdot (g_2 \cdot \varphi))(x) = (g_2 \cdot \varphi)(xg_1) = \varphi(xg_1g_2) = (g_1g_2 \cdot \varphi)(x),$$

这证明了这样给出的确实定义了 G 在 Ind_H^G 上的作用. 称如此得到的 G 的这个表示为从 H 的表示 V 到 G 上的诱导表示. 从 $\mathrm{Ind}_H^G V$ 到 V^S 的同构表明 $\mathrm{Ind}_H^G V$ 的维数是 $|S| \cdot \dim V = \frac{|G|}{|H|} \dim V$.

例如, 如果 $H = 1$, 而 $V = \mathbf{1}$ 是平凡表示, 那么 $\mathrm{Ind}_H^G V$ 是函数 $\varphi : G \to \mathbf{C}$ 的空间. 它有基 φ_h, $h \in G$, 其定义为, 当 $xh = 1$ 时 $\varphi_h = 1$; 而当 $xh \neq 1$ 时 $\varphi_h(x) = 0$. 如果 $g \in G$, 于是我们有 $(g \cdot \varphi_h)(x) = \varphi_h(xg) = \varphi_{gh}(x)$. 由此推出 $\mathrm{Ind}_{\{1\}}^G \mathbf{1}$ 是 G 的正则表示.

注记 I.3.12. — 由子群的表示得到诱导表示是群 G 的表示的主要来源. 它的主要好处之一是非常容易计算出它们的特征标 (参看附录 C, 那里给出了一些应用).

定理 I.3.13. — 设 $H \subset G$ 为两个有限群, $S \subset G$ 是 $H \setminus G$ 的代表系, V 为 H 的一个表示, 而 $W = \mathrm{Ind}_H^G V$. 则对于所有的 $g \in G$ 有

$$\chi_W(g) = \sum_{\substack{s\in S\\ sgs^{-1}\in H}} \chi_V(sgs^{-1}) = \frac{1}{|H|} \sum_{\substack{s\in G\\ sgs^{-1}\in H}} \chi_V(sgs^{-1}).$$

证明 利用 W 与 $V^S = \oplus_{s\in S} V_s$ 的同构. 在此同构下, 如果 φ 是 $(v_s)_{s\in S}$ 的像, 则有 $\varphi(x) = h_x \cdot v_{h_x^{-1}x}$, 而 $g \cdot \varphi$ 是 $((g \cdot \varphi)(s))_{s\in S} = (\varphi(sg))_{s\in S}$, 这使我们得到

$$g \cdot (v_s)_{s\in S} = (h_{sg} \cdot v_{h_{sg}^{-1}sg})_{s\in S}.$$

选取 V 的一组基 $(e_i)_{i\in I}$, 并以 $e_{i,s}$ 记 V^S 的元 $(v_t)_{t\in S}$, 其定义为: $v_s = e_i$ 而当 $t \neq s$ 时 $v_t = 0$. 对于 $i \in I$ 的这些 $e_{i,s}$ 构成了 V_s 的一组基, 而对于 $(i, s) \in I \times S$ 的这些 $e_{i,s}$ 便构成了 V^S 的基. 在这组基下 g 的矩阵是一个以 $(s, s') \in S \times S$ 为下标的分块矩阵, 对应于 (s, s') 的分块是除 $s' = h_{sg}^{-1}sg$ 以外其余全为零的矩阵. 特别

[260] 地, 对迹有所贡献的分块只有那些 $s = h_{sg}^{-1}sg$ 的块, 而它可以写成形如 $h_{sg} = sgs^{-1}$ 的样子. 那么, g 在 V_s 的作用与 $h_{sg} = sgs^{-1}$ 的作用相同, 从而它对迹的贡献是 $\chi_V(sgs^{-1})$. 由此得到定理中的第一个等式. 如果注意到, 当 $h \in H$ 和 $sgs^{-1} \in H$ 时有 $\chi_V(hsg(hs)^{-1}) = \chi_V(h(sgs^{-1})h^{-1}) = \chi_V(sgs^{-1})$, 并且将 $s \in G$ 写为形式 $h_s^{-1}s$, 那么便得到了第二个等式. □

习题 I.3.14. — 用定理 I.3.13 重新证明公式 $\dim(\mathrm{Ind}_H^G V) = \frac{|G|}{|H|}\dim V$.

3.2. 弗罗贝尼乌斯互反公式

设 $H \subset G$ 为两个有限群. 定义线性映射

$$\mathrm{Res}_G^H : R_{\mathbf{C}}(G) \to R_{\mathbf{C}}(H) \quad 和 \quad \mathrm{Ind}_H^G : R_{\mathbf{C}}(H) \to R_{\mathbf{C}}(G)$$

如下: 如果 $\phi \in R_{\mathbf{C}}(G)$, 则 $\mathrm{Res}_G^H\phi$ 就是 ϕ 限制在 H 上的 H 的中心函数; 而如果 $\phi \in R_{\mathbf{C}}(H)$, $\mathrm{Ind}_H^G\phi$ 是由公式

$$(\mathrm{Ind}_H^G\phi)(g) = \frac{1}{|H|}\sum_{\substack{s\in G\\ sgs^{-1}\in H}} \phi(sgs^{-1})$$

给出的 G 上的中心函数. 于是立即得知, 如果 W 是 G 的一个表示, 则 $\mathrm{Res}_G^H\chi_W$ 是只考虑 G 的子群 H 的作用时得到的表示的特征标. 另外, 如果 V 是 H 的一个表示, 则根据定理 I.3.13, $\mathrm{Ind}_H^G\chi_V$ 是诱导表示 $\mathrm{Ind}_H^G V$ 的特征标.

为了区别起见, 分别以 $\langle,\rangle_H$ 和 $\langle,\rangle_G$ 记 $R_{\mathbf{C}}(H)$ 和 $R_{\mathbf{C}}(G)$ 上的标量积. 我们有如下结果.

定理 I.3.15. — (弗罗贝尼乌斯互反公式) 如果 ϕ_1 和 ϕ_2 分别属于 $R_{\mathbf{C}}(H)$ 和 $R_{\mathbf{C}}(G)$, 则

$$\langle\phi_1, \mathrm{Res}_G^H\phi_2\rangle_H = \langle\mathrm{Ind}_H^G\phi_1, \phi_2\rangle_G.$$

证明 由定义知

$$\begin{aligned}\langle\mathrm{Ind}_H^G\phi_1, \phi_2\rangle_G &= \frac{1}{|G|}\sum_{g\in G}\overline{\mathrm{Ind}_H^G\phi_1(g)}\phi_2(g)\\ &= \frac{1}{|G|}\sum_{g\in G}\left(\frac{1}{|H|}\sum_{\substack{s\in G\\ sgs^{-1}\in H}}\overline{\phi_1(sgs^{-1})}\right)\phi_2(g).\end{aligned}$$

令 $h = sgs^{-1}$, 从而 $g = s^{-1}hs$, 那么, 可将上面的和式写为

$$\frac{1}{|H||G|}\sum_{h\in H, s\in G}\overline{\phi_1(h)}\phi_2(s^{-1}hs),$$

[261] 又因为 ϕ_2 是 G 上的中心函数, 故对任意的 $s \in G$ 有 $\phi_2(s^{-1}hs) = \phi_2(h)$. 于是得到

$$\langle \mathrm{Ind}_H^G \phi_1, \phi_2 \rangle_G = \frac{1}{|H|} \sum_{h\in H} \overline{\phi_1(h)} \phi_2(h) = \langle \phi_1, \mathrm{Res}_G^H \phi_2 \rangle_H,$$

定理得证. □

下面是这个定理的一个十分有用的特殊情形.

推论 I.3.16. — 如果 W(分别地, V) 是 G (分别地, H) 的一个不可约表示, 则 W 在 $\mathrm{Ind}_H^G V$ 中的重数等于 V 在 $\mathrm{Res}_G^H W$ 中的重数.

证明　只需对 $\phi_1 = \chi_V$ 和 $\phi_2 = \chi_W$ 应用弗罗贝尼乌斯公式, 并结合推论 I.2.18 即可. □

习题 I.3.17. — (i) 证明, 如果 V, V_1, V_2 是 G 的表示, 则

$$\mathrm{Hom}_G(V, V_1 \oplus V_2) = \mathrm{Hom}_G(V, V_1) \oplus \mathrm{Hom}_G(V, V_2),$$
$$\mathrm{Hom}_G(V_1 \oplus V_2, V) = \mathrm{Hom}_G(V_1, V) \oplus \mathrm{Hom}(V_2, V).$$

(ii) 推导, 如果 V 和 V' 是 G 的两个表示, 则 $\dim(\mathrm{Hom}(V, V') = \langle \chi_V, \chi_{V'} \rangle$.

(iii) 设 H 是 G 的一个子群, 且 W 是 H 的一个表示, 而 V 是 G 的一个表示. 如果 $u \in \mathrm{Hom}_H(W, \mathrm{Res}_G^H V)$, 并以 $\alpha_u : \mathrm{Ind}_H^G W \to V$ 记将 Ind_H^G 的元 $\phi : G \to W$ 映到 $\alpha_u(\phi) = \frac{1}{|G|} \sum_{g\in G} g^{-1} u(\phi(g))$ 的映射. 证明 $\alpha_u \in \mathrm{Hom}_G(\mathrm{Ind}_H^G W, V)$.

(iv) 证明从 $\mathrm{Hom}_H(W, \mathrm{Res}_G^H V)$ 到 $\mathrm{Hom}_G(\mathrm{Ind}_H^G W, V)$ 的映射 $u \mapsto \alpha_u$ 是一个同构 (对于这些表示的弗罗贝尼乌斯互反).

3.3. 诱导表示的传递性

命题 I.3.18. — 设 $K \subset H \subset G$ 为有限群.

(i) 如果 $\phi \in R_{\mathbf{C}}(K)$, 则 $\mathrm{Ind}_H^G(\mathrm{Ind}_K^H \phi) = \mathrm{Ind}_K^G \phi$.

(ii) 如果 W 是 K 的一个表示, 则 $\mathrm{Ind}_H^G(\mathrm{Ind}_K^H W) = \mathrm{Ind}_K^G W$.

证明　考虑到一个表示由它的特征标决定 (推论 I.2.19), 那么 (ii) 就是应用 (i) 到 $\phi = \chi_W$ 的结果. 为证明 (i), 我们从公式

$$\begin{aligned}\mathrm{Ind}_H^G(\mathrm{Ind}_K^H \phi)(g) &= \frac{1}{|H|} \sum_{\substack{s\in G \\ sgs^{-1}\in H}} (\mathrm{Ind}_K^H \phi)(sgs^{-1}) \\ &= \frac{1}{|H|} \sum_{\substack{s\in G \\ sgs^{-1}\in H}} \frac{1}{K} \sum_{\substack{h\in H \\ hsgs^{-1}h^{-1}\in K}} \phi(hsgs^{-1}h^{-1})\end{aligned}$$

出发. 令 $hs = t$ 从而 $s = h^{-1}t$, 这让我们可以将上面的这个和转化为

$$\frac{1}{|H| \cdot |K|} \sum_{\substack{h\in H, t\in G \\ tgt^{-1}\in K, h^{-1}tgt^{-1}h\in H}} \phi(tgt^{-1}).$$

[262] 由于条件 $h^{-1}tgt^{-1}h \in H$ 自动满足, 故如果 $tgt^{-1} \in K$ 且 $h \in H$, 则上面的和可简化成为

$$\frac{1}{|K|} \sum_{\substack{t \in G \\ tgt^{-1} \in K}} \phi(tgt^{-1}) = (\mathrm{Ind}_K^G \phi)(g).$$

得证. □

3.4. 阿廷定理和布饶尔定理

定理 I.3.19. — (阿廷 (Artin), 1930) 设 G 为有限群, V 是 G 的一个表示, 则存在一个非零整数 d_V 和偶对 (C_i, χ_i), $i \in I$ 的有限族, 其中 C_i 是 G 的一个循环子群, 而 $\chi_i \in \widehat{C_i}$ 是 C_i 的一个线性特征标, 使得

$$d_V \chi_V = \sum_{i \in I} n_i \mathrm{Ind}_{C_i}^G \chi_i,$$

其中 $i \in I$, $n_i \in \mathbf{Z}$.

证明　先证明, 对于 C 遍历 G 的循环子群而 χ 遍历 $\widehat{C}$ 的元素时, 这些 $\mathrm{Ind}_C^G \chi$ 构成了 $R_{\mathbf{C}}(G)$ 的一个生成元族. 否则, 存在一个非零的 $\phi \in R_{\mathbf{C}}(G)$ 与 $\mathrm{Ind}_C^G \chi$ 的所有元都正交. 应用弗罗贝尼乌斯互反公式, 得到对任意的 $\chi \in \widehat{C}$ 有 $\langle \phi, \chi \rangle_C = 0$. 令 $c \in G$. 由 c 生成的 G 的子群 C 按定义是个循环群. 由于一个循环群特别是交换的, 那么这些 $\chi \in \widehat{C}$ 生成了 C 到 $\mathbf{C}$ 的函数的向量空间 (推论 I.2.25). 如果 $\phi_C : C \to \mathbf{C}$ 是在 c 取 1 而其余为 0 的函数, 从而有 $0 = \langle \phi, \phi_c \rangle_C = \frac{1}{|C|}\overline{\phi(c)}$, 因此 $\phi(c) = 0$. 由此知 ϕ 恒等于 0, 这便证明了我们的断言, 即这些 $\mathrm{Ind}_C^G \chi$ 构成了 $R_{\mathbf{C}}(G)$ 的一个生成元族.

抽出一组基 $e_i = \mathrm{Ind}_{C_i}^G \chi_i$, $i \in I$. 如果 $\chi \in \mathrm{Irr}(G)$, 由于 $\langle \chi, e_i \rangle \in \mathbf{N}$ 是对应于 χ 的不可约表示在 $\mathrm{Ind}_{C_i}^G \chi_i$ 分解为不可约表示中的重数. 进而, $e_i = \sum_{\chi \in \mathrm{Irr}(G)} \langle \chi, e_i \rangle \chi$. 从基 e_i, $i \in I$ 过渡到基 χ, $\chi \in \mathrm{Irr}(G)$ 的矩阵的系数因而是有理的, 又由于完全同样的理由, χ_V 在基 χ, $\chi \in \mathrm{Irr}(G)$ 下具有整数坐标, 这表明 χ_V 在基 e_i, $i \in I$ 下具有有理坐标. 因此为了得到所要的分解, 只需取 d_V 为 χ_V 在基 e_i, $i \in I$ 下的坐标的分母的最小公倍数即可. 得到结论. □

定理 I.3.20. — (布饶尔 (R. Brauer), 1947) 设 G 为有限群, 而 V 是 G 的一个表示, 则存在一个偶对 (H_i, χ_i), $i \in I$ 的有限族, 其中 H_i 是 G 的子群而 $\chi_i \in \widehat{H_i}$ 是 H_i 的一个线性特征标, 使得

$$\chi_V = \sum_{i \in I} n_i \mathrm{Ind}_{H_i}^G \chi_i, \quad n_i \in \mathbf{Z}, i \in I.$$

[263] 它与阿廷定理的主要差别是没有整数 d_V, 它具有一些非常好的推论(在 §G.1 中提到了其中的一个推论). 另一个差别是它不能限制到循环群上 (布饶尔证明它可以限制到初等群上: 称一个有限群为初等的是说, 存在有限个素数 p 使得 H 是一个 p-群 (阶为 p 的幂的群) 与一个阶与 p 互素的循环群的乘积). 它的证明要用到 $\chi_V(g)$ 的可积性, 这超出了本书的范围. 还应注意, 这些可积性也让我们可以证明下面的结果.

命题 I.3.21. — 如果 G 是有限群, 而 V 是 G 的一个不可约表示, 则 $\dim V$ 整除 $|G|$.

4. 习题

4.1. 特征标表

已知 S_n (分别地, A_n) 代表置换 (分别地, 交错) 群, 参看小词典的 3.4 小节.

习题 I.3.22. — 设 $n \geqslant 1$ 是整数, $\mathbf{Z}/n\mathbf{Z}$ 的不可约表示有哪些?

习题 I.3.23. — 设 G 为 6 阶的非交换群.

(i) G 的元的阶有哪些?

(ii) 证明 G 有两个 1 次的不可约特征标 (记为 $\mathbf{1}$ 和 η) 和一个 2 次不可约特征标 (记为 χ).

(iii) 证明 G 有三个共轭类; 它们是什么?

(iv) 证明, 如果 g 的阶为 3, 则 $\eta(g) = 1$; 而如果 g 的阶为 2, 则 $\eta(g) = -1$(有意思的是 $\eta(g^2)$). 请推出每个共轭类的基数.

(v) 建立 G 的特征标表.

习题 I.3.24. — (i) 证明一个 8 阶的非交换群有四个 1 维和一个 2 维的不可约表示.

(ii) 设 D_4 是正方形的对称群. 证明 D_4 的阶为 8, 并建立 D_4 的特征标表.

(iii) 设 H_4 为四元数群, 它是 $\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$, $\{a, b\} \subset \{0, 1, -1, i, -i\}$ 和 $a = b = 0$ 的集合. 证明 H_4 是一个不同构于 D_4 的 8 阶群, 并建立它的特征标表.

习题 I.3.25. — 让 S_n 在 $\mathbf{C}^n$ 上的作用为置换它的标准基的元. 证明超平面 $\sum_{i=1}^n x_i = 0$ 在 S_n 下稳定且如此得到的表示是不可约的 (考虑 $v - \sigma \cdot v$, 其中的 σ 是一个对换). 由此得到 $\mathbf{C}^n$ 的一个 S_n 的不可约表示的和的分解.

习题 I.3.26. — (o) S_4 的共轭类有哪些?

(i) 证明 $C = \{1, (12)(34), (13)(24), (14)(23)\}$ 是 S_4 的一个正规子群且 $S_4/C = S_3$. (让 S_4 以取共轭作用于 $C - \{1\}$ 上.)

(ii) 因此得到 S_4 的一个 2 维和两个 1 维的不可约表示.

(iii) 让 S_4 以置换标准基作用于 $\mathbf{C}^4$. 证明超平面 $V = \{x_1 + x_2 + x_3 + x_4 = 0\}$ 在 S_4 下稳定, 并计算特征标 χ_V.

(iv) 证明 V 不可约, 并且与 $V \otimes \mathrm{sign}$ 不同构. 由此得到 S_4 的特征标表.

习题 I.3.27. — (o) 证明 S_5 有七个共轭类, 并计算每个类的基数. [264]

(i) 以 U 记 S_5 在 $\mathbf{C}^5$ 的超平面 $\sum_{i=1}^5 x_i$ 上的表示. 计算 χ_U, 并证明 U 和 $U \otimes \mathrm{sign}$ 为不同构的不可约表示.

(ii) 计算 $\chi_{\wedge^2 U}$, 并证明 $\wedge^2 U$ 不可约.

(iii) 计算 $\chi_{\mathrm{Sym}^2 U}$, 并证明 $\mathrm{Sym}^2 U = \mathbf{1} \oplus U \oplus V$, 其中 V 不可约.

(iv) 建立 S_5 的特征标表.

习题 I.3.28. — 设 $n \geqslant 3$, D_n 是具 n 个顶点的正多边形, 而 $C_n \subset D_n$ 是旋转子群.

(i) 证明 C_n 是一个在 D_n 中指数为 2 的循环子群. 证明, 如果 n 是个偶数 (分别地, 奇数), 则对称变换构成两个 (分别地, 一个) 共轭类和旋转 $\frac{n}{2}+1$(分别地, $\frac{n+1}{2}$).

(ii) 证明, 如果将以角 α 的旋转等同于在复平面中以 $e^{i\alpha}$ 所作的乘积, 则 C_n 的不可约表示便是对于所有 $a \in \mathbb{Z}/n\mathbb{Z}$ 的那些 χ_a, 这里 χ_a 的定义为 $\chi_a(e^{i\alpha}) = e^{ai\alpha}$.

(iii) 如果 $a \in \mathbf{Z}/n\mathbf{Z}$, 计算 $\mathrm{Ind}_{C_n}^{D_n}\chi_a$ 的特征标 ϕ_a.

(iv) 计算 $\langle \phi_a, \phi_a \rangle$; 由此推出, 在何种情形下 $\mathrm{Ind}_{C_n}^{D_n}\chi_a$ 是不可约的.

(v) 建立 D_n 的特征标表.

4.2. 更具理论性的习题

习题 I.3.29. — 设 G 为 $\mathbf{GL}_n(\mathbf{C})$ 的一个有限子群. 证明 $\sum_{M \in G} \mathrm{Tr}(M)$ 是一个整数. 如何解释这个整数?

习题 I.3.30. — (i) 如果 $\sigma \in S_n$, 令 $f(\sigma)$ 为置换 σ 的不动点的个数. 证明 $\sum_{\sigma \in S_n} f(\sigma)^2 = 2n!$. (利用习题 I.3.25.)

(ii) S_n 中一个元的不动点的平均个数是多少?

习题 I.3.31. — 如果 $N \geqslant 1$ 是一个整数, 以 $\boldsymbol{\mu}_N$ 记 N 次单位根的集合, 而 $\boldsymbol{\mu}_N^* \subset \boldsymbol{\mu}_N$ 是单位元根的集合, 又令 $S(N) = \sum_{\eta \in \boldsymbol{\mu}_N} \eta$ 和 $S^*(N) = \sum_{\eta \in \boldsymbol{\mu}_N^*} \eta$.

(i) 用 $\boldsymbol{\mu}_{N/d}$, $d \mid N$ 写出 $\boldsymbol{\mu}_N^*$. 由此推出 $S^*(N) = \sum_{d \mid N} \mu(d) S(N/d)$, 其中 $\mu : \mathbf{N} - \{0\} \to \{-1, 0, 1\}$ 为默比乌斯函数, 其定义为: 当 n 被一个素数的平方整除时 $\mu(n) = 0$, 而当是 r 个不同素数的乘积时, $\mu(n) = (-1)^r$.

(ii) 证明 $S^*(N) \in \mathbf{Z}$, 其中 $N \geqslant 1$.

(iii) 设 V 是 S_n 的一个表示, 而 $g \in S_n$ 的阶为 N. 证明 $\rho_V(g)$ 的特征值 (连同重数) 的集合在 $\lambda \mapsto \lambda^k$ 下稳定, 其中 k 为任意与 N 互素的整数. (它涉及将 g^k 循环分解.)

(iv) 由此推出 S_n 的特征标取整数值.

(v) 设 χ 是 S_n 的一个不可约特征标且不同于平凡特征标和 sign. 证明 $\chi(1) \neq 1$, 并由此推出存在 $g \in G$ 使得 $\chi(g) = 0$. (计算 $\langle \chi, \chi \rangle$.)

以下的所有习题中 G 均是有限群.

习题 I.3.32. — 假设 G 以2-可迁的方式作用于 X(这表明对于 X 的元的所有偶对 (x, x'), $x \neq x'$ 和 (y, y'), $y \neq y'$, 存在 $g \in G$ 使得 $g \cdot x = y$, $g \cdot x' = y'$).

(i) 证明稳定子 G_y, $y \in X$ 以可迁的方式作用于 $X - \{y\}$.

(ii) 证明 V_X 的超平面 $W=\{\sum_{x\in X}\lambda_x e_x, \sum_{x\in X}\lambda_x=0\}$ 是 G 的一个不可约表示. (如果 $v=\sum_{x\in X}\lambda_x e_x\in W$, 且 $y\in X$, 则它与 $\frac{1}{|G_y|}\sum_{g\in G_y} g\cdot v$ 有关.)

(iii) 重新得出习题 I.3.25 的结果.

习题 I.3.33. — 如果 χ 是 G 的一个表示的特征标, 令 $K_\chi=\{g\in G, \chi(g)=\chi(1)\}$.

(i) 证明 K_χ 是 G 的一个正规子群.

(ii) 证明 G 为单群当且仅当对所有的 $\chi\in \mathrm{Irr}(G)-\{1\}$ 有 $K_\chi=\{1\}$. 如何从它 [265] 的特征标表上读出一个有限群的单性?

习题 I.3.34. — 设 V 是 G 的一个忠实表示 (即当 $g\neq 1$ 时 $\rho_V(g)\neq 1$).

(i) 证明当 $g\neq 1$ 时 $\chi_V(g)\neq \dim V$.

(ii) 设 W 是 G 的一个不可约表示. 证明 $\sum_{n=0}^{+\infty}\langle \chi_W, \chi_V^n\rangle T^n$ 是一个有显式表达的有理函数, 但不是一个多项式.

(iii) 由此推出 W 出现在 $\oplus^n V$ 的无限处的一个不可约分解中.

习题 I.3.35. — 设 $H\neq G$ 是 G 的一个子群, 而 V 是相伴于 G 在 G/H 上的置换作用的表示.

(i) 证明 $V=\mathrm{Ind}_H^G \mathbf{1}$. 由此得到 $\sum_{g\in G}\chi_V(g)=|G|$.

(ii) 证明 V 不是不可约的; 由此得到 $\frac{1}{|G|}\sum_{g\in G}\chi_V(g)^2\geqslant 2$. (注意 χ_V 是实的.)

(iii) 设 Y 是满足 $\chi_V(g)=0$ 的 $g\in G$ 的集合. 证明

$$\sum_{g\in G}(\chi_V(g)-1)(\chi_V(g)-|G/H|)\leqslant |G/H|\cdot|Y|.$$

(iv) 由此推导出 $|Y|\geqslant |H|$.

(v) 设 X 是满足 $|X|\geqslant 2$ 的一个集合, 而 G 可迁地作用其上 (即对任意的 $x,y\in X$, 存在 $g\in G$ 使得 $y=g\cdot x$). 证明那些作用在 X 上无不动点的 $g\in G$ 部分的比例大于[10]或等于 $1/|X|$.

习题 I.3.36. — 设 G_1, G_2 为两个有限群, 并令 $G=G_1\times G_2$.

(i) 证明, 如果 V_1 和 V_2 分别是 G_1 和 G_2 的不可约表示, 则 $V_1\boxtimes V_2$(参看 I.3.6) 是 G 的一个不可约表示.

(ii) 证明 G 的所有不可约表示都可按此方式得到.

习题 I.3.37. — (i) 如果 $\sigma\in S_n$, 而 M_σ 是将 $\mathbf{C}^n$ 的标准基中的 e_i 映到 $e_{\sigma(i)}$ 的同构 u_σ 的矩阵. 按照 σ 的循环分解, M_σ 的特征值 (带重数) 是什么? 由此推出, 如果 M_σ 和 M_τ 相似, 则 σ 和 τ 具有相同个数的不动点.

(ii) 证明有 G 的特征标表定义的矩阵 T_G 可逆.

---

[10] 在代数数论中, 这个属于若尔当的结果让我们可以证明, 如果 $P\in\mathbf{Z}[T]$, $\deg P\geqslant 2$ 在 $\mathbf{Q}[T]$ 中不可约, 则存在无穷多个素数 p 使得 P 在 $\mathbf{F}_p$ 中无解.

(iii) 证明, 如果 $C \in \mathrm{Conj}(G)$, 则 $C^{-1} = \{g^{-1}, g \in C\}$ 属于 $\mathrm{Conj}(G)$, 且若 $\chi \in \mathrm{Irr}(G)$, 则 $\chi(C^{-1}) = \overline{\chi(C)}$.

(iv) 证明 G 的对称共轭类 (即满足 $C = C^{-1}$) 的个数等于 G 的实特征标 (即对于所有 $C \in \mathrm{Conj}(G)$ 有 $\chi(C) \in \mathbf{R}$) 的个数.

II. 巴拿赫空间

[267]

完备的赋范向量空间的理论 (由于巴拿赫在该理论的形成中所起的作用也被称作 "巴拿赫空间") 起源于 19 世纪的关于微分方程、偏微分方程或者形如 $u(x)+\int_a^b K(x,y)u(y)dy=f(x)$ 的积分方程, 其中的 u 是个未知量. 从它到希尔伯特 (1906) 引进了冠以他名字的空间 (平方可和序列的空间 ℓ^2) 之间花去了 20 年, 随后数年, 菲舍尔 (Fischer) 和里斯 (Riesz) 建立了与它同构的平方可和函数的空间, 而这个理论的最终形式由波兰学派完成 (S. 巴拿赫, H. 哈恩 (Hahn), H. 施泰豪斯 (Steinhaus)). 反过来, 这个理论对于原来的那些问题的解决也有很多的好处. 巴拿赫空间的分类一直是个基本问题[1].

II.1. 巴拿赫空间

后面 $\mathbf{K}$ 或是代表实数域 $\mathbf{R}$[2], 或是代表复数域 $\mathbf{C}$, 而 "向量空间" 是 "$\mathbf{K}$ 上的向量空间" 的简略说法. 读者可以返回到小词典的 §17 参看赋范空间的词条和它们的初等性质.

1. 按范数的收敛性, 可和级数

设 $(E,\|\ \|)$ 为一个赋范向量空间. 回忆, 如果 $x\in E$, $r\in\mathbf{R}_+$, 我们以 $B(x,r)$ 或 $B_E(x,r)$(分别地, $B(x,r^-)$ 或 $B_E(x,r^-)$) 表示中心为 x, 半径为 r 的闭 (分别地, [268]

---

[1] 长时间一直没有解决的问题是 $\mathbf{C}$-巴拿赫空间的自同态是否总具有一个闭的不变子空间 (是指有限维 $\geqslant 2$ 的情形). 到 1981 年 P. Enflo 构造了一个反例, 而 C. Read (1984) 在可和序列空间 ℓ^1 中也构造了一个, 但我们仍然不知道在 ℓ^2 中, 或更一般地在不是 ℓ^1 的自反空间中是否存在反例.

[2] 或者, 更一般地, 对某个完备的赋范空间 K(参看小词典的 17.1 小节). 唯一常常不能推广的命题是哈恩 – 巴拿赫定理 (定理 II.1.29). 但我们并不打算证明它.

开) 球.

称 E 中的元的一个级数 $\sum_{n\in\mathbf{N}} u_n$ 按范数收敛是说有 $\sum_{n\in\mathbf{N}} \|u_n\| < +\infty$.

称完备的赋范向量空间 $(E, \|\ \|)$(按照与此范数相伴的距离完备) 为巴拿赫空间. 根据小词典的 14.1 小节, $(E, \|\ \|)$ 是巴拿赫空间当且仅当所有按范数收敛的级数均收敛于 E 中. 由于完备空间的闭子空间仍然完备, 故巴拿赫空间的闭子向量空间仍为巴拿赫空间.

最简单的一些巴拿赫空间的例子是有限维的, 然而它们具有非常特殊的一些性质. 我们特别有如下的一些经典的结果 (参看小词典的 17.4 和 17.5 小节).

命题 II.1.1. — (i) 如果 V 是有限维向量空间, 则 V 上的所有范数都等价, 并且 V 在其中任一个下都是完备的.

(ii) 设 V 是巴拿赫空间, 单位闭球 $B(0,1)$ 为紧的当且仅当 E 为有限维的.

注记 II.1.2. — 我们强调, 命题 II.1.1 的 (i) 在无限维的情形是完全错误的: 无限维的空间 V 上的范数并非总是等价的, E 可能对它们中某些是完备的但它们中 "更多的" 不是这样的.

称一个空间是可分的是指它包含了一个稠的可数子集[3](即如果它 "不太大").

习题 II.1.3. — (i) 证明有限维向量空间是可分的.

(ii) 证明可分空间的子空间是可分的.

设 E 为巴拿赫空间. 称一个级数 $\sum_{i\in I} x_i$, 其中 I 可数, 为可和的是说它满足下面的与排序无关的柯西判别准则: 对于 $\forall\varepsilon > 0$, 存在有限的 $I(\varepsilon) \subset I$ 使得满足 $J \cap I(\varepsilon) = \varnothing$ 的所有有限子集 $J \subset I$ 有 $\|\sum_{i\in J} x_i\| \leqslant \varepsilon$.

- 如果 I 有限, 所有的级数 $\sum_{i\in I} x_i$ 可和.
- 如果 I 无限, 且若 $\sum_{i\in I} x_i$ 可和, 则对于每个双射 $n \mapsto i(n) : \mathbf{N} \to I$, 级数 $\sum_{n=0}^{+\infty} x_{i(n)}$ 的部分和满足通常的柯西判别准则, 并且, 由于 E 完备, 故此级数收敛, 其极限不依赖双射 $n \mapsto i(n)$ 的选取; 称它是级数 $\sum_{i\in I} x_i$ 的和.

可和性与按范数的收敛性是十分相近的概念. 下面的习题 (在其中感兴趣的是级数 $\sum_{i\in I} x_i$, 这里的 I 是无限可数集) 研究了它们间的联系.

[269] **习题 II.1.4.** — (i) 证明一个按范数收敛的级数可和.

(ii) 证明在 $\mathbf{R}$ 中一个级数可和当且仅当它是绝对收敛的.

(iii) 由此推出, 在一个有限维的在 $\mathbf{R}$ 或 $\mathbf{C}$ 上的赋范向量空间中, 一个级数可和当且仅当它是按范数收敛的.

(iv) 设 I 可数 (下面将定义空间 $\ell^2(I)$ 和 $\ell^\infty(I)$), 且对 $i \in I$, 令 e_i 为 $\mathbf{C}$ 中级数

[3] 泛函分析中的大部分巴拿赫空间是可分的; 值得注意的一个例外是空间 $\mathscr{C}_b(\mathbf{R})$, 即 $\mathbf{R}$ 上的有界连续函数的空间 (参看习题 II.1.7) 或者有界序列的空间 ℓ^∞.

$(e_{i,j})_{j\in I}$, 其中 $e_{i,i}=1$, 而当 $i\neq j$ 时 $e_{i,j}=0$.

(a) 证明 $\sum_{i\in I} a_i e_i$ 在 $\ell^\infty(I)$ 中可和当且仅当级数 $(a_i)_{i\in I}$ 在无穷远处收敛于 0 (对于 $\forall\varepsilon>0$, 存在有限集 $I(\varepsilon)\subset I$ 使得当 $i\notin I(\varepsilon)$ 时 $|a_i|\leqslant\varepsilon$).

(b) 证明 $\sum_{i\in I} a_i e_i$ 在 $\ell^2(I)$ 中可和当且仅当 $\sum_{i\in I}|a_i|^2<+\infty$.

(c) 这两种情形下的和是什么?

2. 序列空间

例题 II.1.5. — (i) 以 ℓ^∞ 记有界序列 $(x_n)_{n\in\mathbf{N}}$ 的集合. 在其上赋予范数 $\|\ \|_\infty$: $\|(x_n)_{n\in\mathbf{N}}\|_\infty=\sup_{n\in\mathbf{N}}|x_n|$, 则空间 ℓ^∞ 是一个巴拿赫空间. ℓ^∞ 的子空间 ℓ_0^∞ 由当 n 趋向 $+\infty$ 时趋向 0 的序列组成, 它是 ℓ^∞ 的一个闭子空间, 从而也是一个巴拿赫空间.

(ii) 以 ℓ^1 记满足 $\sum_{n\in\mathbf{N}}|x_n|<+\infty$ 的序列 $(x_n)_{n\in\mathbf{N}}$ 组成的空间. 赋予范数 $\|\ \|_1:\|(x_n)_{n\in\mathbf{N}}\|_1=\sum_{n\in\mathbf{N}}|x_n|$, 则空间 ℓ^1 是一个巴拿赫空间.

(iii) 以 ℓ^2 记满足 $\sum_{n\in\mathbf{N}}|x_n|^2<+\infty$ 的序列 $(x_n)_{n\in\mathbf{N}}$ 的集合. 赋予范数 $\|\ \|_2$: $\|(x_n)_{n\in\mathbf{N}}\|_2=(\sum_{n\in\mathbf{N}}|x_n|^2)^{1/2}$. 则空间 ℓ^2 是一个巴拿赫空间[(4)].

(iv) 如果 I 是一个无限可数集, 于是可同样定义空间 $\ell^\infty(I),\ell_0^\infty(I),\ell^1(I),\ell^2(I)$; 它们也是巴拿赫空间.

证明　I 为可数的情形可由 $\mathbf{N}$ 的情形得到, 这只需选取一个从 I 到 $\mathbf{N}$ 的双射即可; 因而只要证明 (i),(ii) 和 (iii). 设 E 为 ℓ^∞, ℓ^1, ℓ^2 中的一个, 并设 $\|\ \|$ 为它们相应的范数. 为了证明 E 是一个巴拿赫空间, 需要证明所有按范数收敛的 E 中级数在 E 中有一个极限. 令 $(x^{(k)})_{k\in\mathbf{N}}$ 是 E 中的一个序列, 满足 $\sum_{k\in\mathbf{N}}\|x^{(k)}\|<+\infty$. 每个 $x^{(k)}$ 是 $\mathbf{K}$ 中的一个序列 $(x_n^{(k)})_{n\in\mathbf{N}}$, 在这三种情形对每个 $n\in\mathbf{N}$ 都有 $|x_n^{(k)}|\leqslant\|x^{(k)}\|$, 这表明对于任意的 $n\in\mathbf{N}$, 级数 $\sum_{k\in\mathbf{N}}x_n^{(k)}$ 在 $\mathbf{K}$ 中按范数收敛, 从而在 $\mathbf{K}$ 中收敛 (因为 $\mathbf{K}$ 完备); 我们以 y_n 记此级数和, 而以 y 记序列 $(y_n)_{n\in\mathbf{N}}$. 要得到结论, 只需证明 $\|y\|\leqslant\sum_{k\in\mathbf{N}}\|x^{(k)}\|$ 即可: 事实上, 这证明了 $y\in E$, $\|y-\sum_{i\leqslant k}x^{(i)}\|\leqslant\sum_{i\geqslant k+1}\|x^{(i)}\|$ 当 $k\to+\infty$ 时趋向 0: 它被一个收敛级数的余项所控制, 因此 y 是级数 $\sum_{k\in\mathbf{N}}x^{(k)}$ 在 E 中的和.

- 如果 $E=\ell^\infty$, 则有 $|y_n|\leqslant\sum_{k\in\mathbf{N}}|x_n^{(k)}1\leqslant\sum_{k\in\mathbf{N}}\|x^{(k)}\|_\infty$, 因此 $\|y\|_\infty\leqslant\sum_{k\in\mathbf{N}}\|x^{(k)}\|_\infty$. 至于 ℓ_0^∞ 在 ℓ^∞ 中的闭性, 请参看小词典的习题 16.2.
- 如果 $E=\ell^1$, 则有 $|y_n|\leqslant\sum_{k\in\mathbf{N}}|x_n^{(k)}|$, 因此 [270]

$$\|y\|_1=\sum_{n\in\mathbf{N}}|y_n|\leqslant\sum_{n\in\mathbf{N}}\sum_{k\in\mathbf{N}}|x_n^{(k)}|=\sum_{k\in\mathbf{N}}\sum_{n\in\mathbf{N}}|x_n^{(k)}|=\sum_{k\in\mathbf{N}}\|x^{(k)}\|_1.$$

- 如果 $E=\ell^2$, 则有

$$\sum_{n\in\mathbf{N}}|y_n|^2\leqslant\sum_{n\in\mathbf{N}}(\sum_{k\in\mathbf{N}}|x_n^{(k)}|)^2=\sum_{n\in\mathbf{N}}\sum_{k_1,k_2\in\mathbf{N}}|x_n^{(k_1)}||x_n^{(k_2)}|$$

[(4)]由于范数 $\|\ \|_2$ 由标量积定义, 故它同样是一个希尔伯特空间.

$$= \sum_{k_1,k_2\in\mathbf{N}} \sum_{n\in\mathbf{N}} |x_n^{(k_1)}||x_n^{(k_2)}| = \sum_{k_1,k_2\in\mathbf{N}} \langle |x^{(k_1)}|, |x^{(k_2)}| \rangle$$
$$\leqslant \sum_{k_1,k_2\in\mathbf{N}} \|x^{(k_1)}\|_2 \|x^{(k_2)}\|_2 = (\sum_{k\in\mathbf{N}} \|x^{(k)}\|_2)^2,$$

其中我们用到了如下几个事实: 在一个正项级数中可以随意重排序; 记号 $|x^{(k)}|$ 代表了序列 $(|x_n^{(k)}|)_{n\in\mathbf{N}}$; 以及柯西 – 施瓦茨公式 (小词典的 18 小节). 由此得到 $\|y\|_2 \leqslant \sum_{k\in\mathbf{N}} \|x^{(k)}\|_2$.

得到结论. □

3. 连续函数空间

如果 X 是拓扑空间, 以 $\mathscr{C}(X)$ 记从 X 到 $\mathbf{C}$ 的连续函数的空间.

例题 II.1.6. — (i) 如果 X 是度量空间 (或更一般地, 一个拓扑空间), 则可赋予 X 到 $\mathbf{C}$ 的有界连续函数的空间 $\mathscr{C}_b(X)$ 一个一致收敛性范数 $\|\ \|_\infty : \|\phi\|_\infty = \sup_{x\in X} |\phi(x)|$. 于是 $(\mathscr{C}_b(X), \|\ \|_\infty)$ 是一个巴拿赫空间. 事实上, $\mathscr{C}_b(X)$ 的完备性是连续函数的一致收敛的极限仍是连续这个性质 (参看小词典 16.2 小节) 的转化.

(ii) 以 $\mathscr{C}_c(X)$ 记 X 上在一个紧集外为零的连续函数的空间 (下标 "c" 代表 "具紧支集"). 由于一个紧集上的连续函数的像为紧集, 从而有界, 故 $\mathscr{C}_c(X) \subset \mathscr{C}_b(X)$, 除了 X 为紧集外这个包含关系是严格的, 而在紧集的情形则有 $\mathscr{C}_c(X) = \mathscr{C}_b(X) = \mathscr{C}(X)$. 以 $\mathscr{C}_0$ 记 $\mathscr{C}_c$ 在 $\mathscr{C}_b$ 的闭包; 这是 X 上在无穷处趋向 0 的连续函数的空间.

(iii) 更一般地, 如果 W 是一个具有范数 $\|\ \|$ 的有限维的 $\mathbf{K}$-向量空间, X 到 W 的有界连续函数的空间 $\mathscr{C}_b(X,W)$ 在范数 $\|\ \|_\infty : \|\phi\|_\infty = \sup_{x\in X} \|\phi(x)\|$ 下是一个巴拿赫空间. 事实上, 由于 W 上的范数都等价, 故改变 W 上的范数等于改变 $\mathscr{C}_b(X,W)$ 上的范数 $\|\ \|_\infty$ 为一个等价的范数; 因此我们可以选取 W 的一组基 $e_1,\dots,e_n$, 并设 $\|\ \|$ 由 $\|x_1e_1+\cdots+x_ne_n\| = \sup_{1\leqslant i\leqslant n} |x_i|$ 给出. 于是每个 $\phi\in\mathscr{C}_b(X,W)$ 可以以唯一的方式写为 $\phi = \sum_{i=1}^n \phi_i e_i$, 其中 $\phi_i \in \mathscr{C}_b(X,\mathbf{K})$, 而 $\phi \mapsto (\phi_1,\dots,\phi_n)$ 是 $\mathscr{C}(X,W)$ [271] 到 $(\mathscr{C}_b(X,\mathbf{K}))^n$ 的同构, 由于完备空间的积仍为完备的, 故它为完备的.

习题 II.1.7. — 如果 $\lambda\in\mathbf{R}$, 以 e_λ 记函数 $t\mapsto e^{2i\pi\lambda t}$.

(i) 证明 $e_\lambda \in \mathscr{C}_b(\mathbf{R})$, 以及当 $\lambda\neq\mu$ 时 $\|e_\lambda - e_\mu\|_\infty = 2$.

(ii) 由此推出 $\mathscr{C}_b(\mathbf{R})$ 不是可分的.

定理 II.1.8. — (斯通 – 魏尔斯特拉斯, 1948) 如果 X 为紧空间, 且 $\mathscr{A}$ 为 $\mathscr{C}(X)$ 的一个包含了常值函数的子代数, 它分离点并且在 $f\mapsto\bar{f}$ 下稳定, 那么, $\mathscr{A}$ 则在 $\mathscr{C}(X)$ 中稠密.

证明　在给出这个重要定理的证明前, 我们来厘清 "$\mathscr{A}$ 分离点" 这个条件: 它表明, 如果 $x\neq y$, 则可找到 $f\in\mathscr{A}$ 使得 $f(x)\neq f(y)$.

现在不妨将 $\mathscr{A}$ 换成它在 $\mathscr{C}(X)$ 中的闭包, 它仍然是满足定理中条件的一个代数, 于是可以假定 $\mathscr{A}$ 是完备的, 因而我们应该证明 $\mathscr{A}=\mathscr{C}(X)$.

令 $\mathscr{A}_{\mathbf{R}}=\mathscr{A}\cap\mathscr{C}(X,\mathbf{R})$. 这是 $\mathscr{C}(X,\mathbf{R})$ 的一个闭子代数 (从而完备), 是取值于 $\mathbf{R}$ 的 X 上的连续函数的集合, 而条件 "$\mathscr{A}$ 在 $f\mapsto\bar{f}$ 下稳定" 导致 $\mathscr{A}_{\mathbf{R}}$ 分离点: 因为当 $f\in\mathscr{A}$ 时, $\mathscr{A}_{\mathbf{R}}$ 便包含了 $\mathrm{Re}(f)=\frac{1}{2}(f+\bar{f})$ 和 $\mathrm{Im}(f)=\frac{1}{2i}(f-\bar{f})$. 因为 $\mathscr{C}(X)=\mathscr{C}(X,\mathbf{R})+i\mathscr{C}(X,\mathbf{R})$, 故只需证明 $\mathscr{A}_{\mathbf{R}}=\mathscr{C}(X,\mathbf{R})$ 即可. 我们需要下面的引理.

引理 II.1.9. — *存在一个实系数的多项式的序列 $(P_n(t))_{n\in\mathbf{N}}$, 它在 $[-1,1]$ 上一致地趋向 $|t|$.*

证明　带余项的泰勒公式

$$f(x)=f(0)+xf'(0)+\cdots+\frac{x^n}{n!}f^{(n)}(0)+\frac{x^{n+1}}{n!}\int_0^1(1-t)^n f^{(n+1)}(tx)dt$$

让我们可以证明, 如果 $\alpha>0$, 则级数 $\sum_{n=0}^{+\infty}\frac{\alpha(\alpha-1)\dots(\alpha-n+1)}{n!}x^n$ 在 $x\in[-1,1]$ 上一致地趋向 $(1+x)^\alpha$. 特别地, 对于 $\alpha=\frac{1}{2}$, $x=t^2-1$, 这个级数的这些部分和给出了在 $[-1,1]$ 上一致趋向 $(1+t^2-1)^{1/2}=|t|$ 的多项式序列. □

回到定理的证明.

- 如果 $f\in\mathscr{A}_{\mathbf{R}}$, 则存在 $a\in\mathbf{R}_+^*$ 使得 f 在 $[-a,a]$ 中取值. 于是 $aP_n(a^{-1}f)$ 是 $\mathscr{A}_{\mathbf{R}}$ 中元的序列, 它一致地趋向 $|f|$, 并且由于 $\mathscr{A}_{\mathbf{R}}$ 完备, 故而当 $f\in\mathscr{A}_{\mathbf{R}}$ 时也有 $|f|\in\mathscr{A}_{\mathbf{R}}$.
- 现在, 如果 $f,g\in\mathscr{A}_{\mathbf{R}}$, 则从上面得到 $\sup(f,g)=\frac{f+g}{2}+\frac{|f-g|}{2}$ 和 $\inf(f,g)=\frac{f+g}{2}-\frac{|f-g|}{2}$ 这两个都属于 $\mathscr{A}_{\mathbf{R}}$.
- 设 $h\in\mathscr{C}(X,\mathbf{R})$. 固定一个 $x\in X$, 以及一个 $\varepsilon>0$. 由于 $\mathscr{A}_{\mathbf{R}}$ 分离点并包含了常值函数, 故对任意的 $y\in X$ 可找到一个函数 $f_y\in\mathscr{A}_{|R}$ 满足 $f_y(x)=h(x)$, $f_y(y)=h(y)$. 由于 $h-f_y$ 连续, 故存在一个包含 y 的开集 U_y 使得对于 $z\in U_y$ 有 $|h(z)-f_y(z)|<\varepsilon$. 因为 X 是紧空间, 而且 U_y 覆盖了 X, 故可选取 X 的一个有限子集 Y 使得 $X=\cup_{y\in Y}U_y$. 因此根据上一个 • 知 $g_x=\inf_{y\in Y}f_y$ 是 $\mathscr{A}_{\mathbf{R}}$ 中的一个元, 且 g_x 满足 $g_x(x)=h(x)$, 而对于任意的 $z\in X$ 有 $g_x(z)\leqslant h(z)+\varepsilon$: 因为 z 至少属于 U_y, $y\in Y$ 中的一个. [272]
- 由于 $g_x(x)=h(x)$ 并且 g_x 连续, 故存在一个包含 x 的开集 V_x 使得当 $z\in V_x$ 时有 $|g_x(z)-h(z)|\leqslant\varepsilon$. 由上面得知, 我们可以从 X 的 V_x 覆盖中抽出一个有限的子覆盖 $(V_x)_{x\in X'}$, 其中 X' 有限. 由上面得知, 函数 $g=\sup_{x\in X'}g_x$ 属于 $\mathscr{A}_{\mathbf{R}}$, 且对于每个 z 有 $g(z)\leqslant h(z)+\varepsilon$: 因为这个不等式对于所有的 g_x 都满足; 又因为 z 至少属于一个 U_x, $x\in X'$, 故 $g(z)\geqslant h(z)-\varepsilon$.

因此, 对于任意的 $\varepsilon>0$ 我们已经构造了 $\mathscr{A}_{\mathbf{R}}$ 中的一个元 g 满足 $\|g-h\|_\infty\leqslant\varepsilon$, 这证明了 h 在 $\mathscr{A}_{\mathbf{R}}$ 的闭包里, 从而在 $\mathscr{A}_{\mathbf{R}}$ 中. 证毕. □

例题 II.1.10. — (i) 如果 I 是 $\mathbf{R}$ 的一个紧区间, 则多项式在 $\mathscr{C}(I)$ 中稠密 (魏尔斯特

拉斯, 1885).

(ii) 更一般地, 如果 K 是 $\mathbf{R}^m$ 的一个紧集, 则 $(x_1,\ldots,x_n)$[5]的多项式在 $\mathscr{C}(K)$ 中稠密.

(iii) 三角多项式 (即形如 $\sum_{k\in I} a_k e^{2i\pi kt}$ 的函数, 其中 I 是遍历 $\mathbf{Z}$ 的有限子集) 在连续的周期为 1 的函数的空间 $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ 中稠密 (魏尔斯特拉斯). 但它们不稠于 $\mathscr{C}([0,1])$: 因为其闭包中的元满足 $f(0)=f(1)$, 故点 0 与 1 不能被三角多项式分离.

习题 II.1.11. — 设 $h:\mathbf{R}\to\mathbf{R}$ 是 $\mathbf{Q}$ 的特征函数.

(i) 构造从 $\mathbf{R}$ 到 $\mathbf{R}$ 的连续函数的二重序列 $f_{n,k}$ 使得, 当 n 固定时, 序列 $f_{n,k}$ 当 k 趋向 $+\infty$ 时简单地趋向函数 g_n (即对于任意的 $x\in\mathbf{R}$ 有 $f_{n,k}(x)\to g_n(x)$), 而序列 g_n 当 n 趋向 $+\infty$ 时简单地趋向 h. (简短地说, 即 h 是连续函数的简单极限的简单极限.)

(ii) 证明 h 不是连续函数的简单极限. (如果 h_n 是一个简单地趋向 h 的连续函数序列, 构造一个子序列 $h_{\varphi(n)}$ 和区间套的序列 $[a_n,b_n]$ 使得 $[a_n,b_n]$ 在 $h_{\varphi(n)}$ 下的像包含在 $[\frac{1}{4},\frac{3}{4}]$ 中, 从而引出矛盾.)

4. 线性微分方程

4.1. 柯西 – 利普希茨定理

设 V 是个有限维的 $\mathbf{K}$-向量空间. 赋予 V 一个范数 $\|\ \|$, 并赋予 $\mathrm{End}(V)$ 以与其相伴的算子范数 (参看小词典的 17.3 小节; 它特别是 $\mathbf{K}$-向量空间的范数而且当 $u\in\mathrm{End}(V)$, $v\in V$ 时有 $\|u(V)\|\leqslant\|u\|\|v\|$).

[273] 令 I 为 $\mathbf{R}$ 的一个区间, $u:I\to\mathrm{End}(V)$ 是一个连续函数. 我们要解微分方程组 $\phi'=u\cdot\phi$, 即描述出属于 $\mathscr{C}^1$ 类的 $\phi:I\to V$ 中使得 $\phi'(t)=u(t)\cdot\phi(t)$ 的集合.

定理 II.1.12. — (柯西 – 利普希茨) *微分方程组 $\phi'=u\cdot\phi$ 的解的集合 $\mathscr{L}$ 是一个 $\dim V$ 维的向量空间, 且映射 $\phi\mapsto\phi(t)$ 对每个 $t\in I$ 诱导了从 $\mathscr{L}$ 到 V 上的一个同构. 换句话说,*

- *如果 $t_0\in I$, 则对于每个 $z\in V$ 在整个 I 上存在微分方程组 $\phi'=u\cdot\phi$ 的一个唯一的解 ϕ_z, 它在 t_0 取值 z;*
- *如果 $t\in I$, 则存在 $a(t)\in\mathrm{GL}(V)$ 使得对所有的 $z\in V$ 有 $\phi_z(t)=a(t)\cdot z$ (其中 $a(t_0)=\mathrm{id}$).*

证明　由取导数和 $u(t):V\to V$ 的线性性知所有解的线性组合仍是解, 从而 $\mathscr{L}$ 是一个向量空间. 由于 $\phi\mapsto\phi(t)$ 显然的线性性, 故只需证明第二个断言 (在 t_0 取值 z 的解的存在性和唯一性); 其余的均可由此推出.

---

[5]注意事实: 如果 D 是 $\mathbf{C}$ 的一个单位圆盘, 则 z 的多项式并不在 $\mathscr{C}(D)$ 中稠密; 事实上, 我们以后会看到, 闭包中的一个元素是一个全纯函数. 问题出在 z 的多项式在 $f\mapsto\bar{f}$ 下不稳定.

条件 "ϕ 属于 $\mathscr{C}^1$ 类" "$\phi' = u\cdot\phi$" 和 "$\phi(t_0) = z$" 等价于 "ϕ 连续" 且 "$\phi(t) = z + \int_{t_0}^t u(x)\cdot\phi(x)dx$". 事实上, ϕ 的连续性导出了 $t\mapsto\int_{t_0}^t u(x)\phi(x)dx$ 的可微与等式 $\phi'(t) = u(t)\cdot\phi(t)$. 换而言之, ϕ 满足前三个条件当且仅当它为连续的且是在 $\phi\mapsto F(\phi)$ 下的不动点, 其中 $F:\mathscr{C}(I,V)\to\mathscr{C}(I,V)$ 由 $(F(\phi))(t) = z + \int_{t_0}^t u(x)\phi(x)dx$ 定义. 因此只要证明 F 在 $\mathscr{C}(I,V)$ 有唯一的不动点即可, 为此, 只要证明将 I 换作一个任意的紧区间 $J\subset I$ 时的相同论断即可 (可将 I 写成紧区间 J_n 的递增并, 而在 J_n 上一个解 $\phi_{z,n}$ 的唯一性表明在 J_{n+1} 上的解 $\phi_{z,n+1}$ 在 J_n 上的限制等于 $\phi_{z,n}$, 因而这些 $\phi_{z,n}$ 给出了方程 $\phi' = u(t)\phi$ 在整个 I 上的解 ϕ_z; 这个解满足 $\phi_z(t_0) = z$, 并在每个 J_n 上也唯一). 以 F^n 代表 n 个 F 的复合 $F\circ\cdots\circ F$.

令 J 为 I 的一个包含 t_0 的紧区间, 并设 $A_J = \sup_{t\in J}\|u(t))\|$. 如果 $\phi: J\to V$ 是一个连续函数, 令 $\|\phi\|_J = \sup_{t\in J}\|\phi(t)\|$, 使得 $\mathscr{C}(J,V)$ 成为一个巴拿赫空间 (参看习题 II.1.6). 我们有

$$\|(F(\phi_1))(t)-(F(\phi_2))(t)\| \leqslant \left|\int_{t_0}^t \|u(x)\|\|\phi_1(x)-\phi_2(x)\|dx\right| \leqslant A_J\left|\int_{t_0}^t \|\phi_1(x)-\phi_2(x)\|dx\right|.$$

$\|\phi_1(x)-\phi_2(x)\|$ 对所有的 $x\in J$ 被函数 $\|\phi_1-\phi_2\|_j$ 囿于上, 这给了我们对于每个 $t\in J$ 一个强函数 $\|(F(\phi_1))(t)-(F(\phi_2))(t)\| \leqslant A_J\|\phi_1-\phi_2\|_J|t-t_0|$. 于是可将此强函数带到上面的不等式中并稍作归纳便证明了, 对于每个 $t\in J$ 有 $\|(F^n(\phi_1))(t)-(F^n(\phi_2))(t)\|_J \leqslant A_J^n\|\phi_1-\phi_2\|_J\frac{|t-t_0|^n}{n!}$. 如果 $M_J = \sup_{t\in J}|t-t_0|$, 则得到 $\|F^n(\phi_1)-F^n(\phi_2)\|_J \leqslant \frac{(A_JM_J)^n}{n!}\|\phi_1-\phi_2\|_J$. 由于 $\frac{(A_JM_J)^n}{n!}\to 0$, 这证明了 F 最多只有一个不动点 (应用取强函数的过程到 F 的两个不动点上). 我们也可应用这个强化过程到 $\phi_1 = F(\phi)$ 和 $\phi_2 = \phi$ 上, 并由于 $\sum_{n\in\mathbf{N}}\frac{(A_JM_J)^n}{n!} < +\infty$, 得到 $\sum_{n\in\mathbf{N}}(F^{n+1}(\phi)-F^n(\phi))$ 是按范数收敛的, 但因 $\mathscr{C}(J,V)$ 完备, 故收敛. 部分和的序 [274] 列从而有极限, 而 $F^n(\phi)$ 对于每个 $\phi\in\mathscr{C}(J,V)$ 都有极限. 因为这个极限是 F 的一个不动点. 从而得到结论. □

注记 II.1.13. — (i) 如果 I' 是 I 的一个开子区间, 由此定理得知在 I' 上的限制诱导了从 I 上的解空间到 I' 上的解空间的同构; 换句话说, I' 上的每个解均可以唯一的方式延拓为 I 上的解.

(ii) 我们已经证明了从任意一个 ϕ 开始, 通过迭代映射 $\phi\mapsto F(\phi)$ 可以得到解 ϕ_z. 例如, 微分方程 $\phi' = \phi$ 在 $\mathbf{R}$ 上有一个维的在 0 取值为 1 的解, 而我们是从任意一个 ϕ 出发通过迭代泛函 $\phi\mapsto 1+\int_0^t\phi(x)dx$ 得到这个解的; 如果从 $\phi = 0$ 出发, 我们得到这些函数是 $1, 1+t, \ldots, 1+t+\frac{t^2}{2}+\cdots+\frac{x^n}{n!}$, 从而解为 $t\mapsto\sum_{n=0}^{+\infty}\frac{t^n}{n!} = e^t$.

(iii) 更一般地, 如果 $I = \mathbf{R}$, 而 $t\mapsto u(t)$ 为常值, 那么由这个不动点方法得到解 ϕ_z 是 $\sum_{n=0}^{+\infty}\frac{t^nu^n}{n!}\cdot z$, 其中我们以指数形式表述 n 重的同一个自同态的复合. 如果我们定义一个自同态 φ 的指数e^φ 为 $e^\varphi = \sum_{n=0}^{+\infty}\frac{\varphi^n}{n!}$(此级数的按范数的收敛性由 $\|\ \|$ 是在 $\mathrm{End}(V)$ 上的一个代数的范数得到, 从而 $\|u^n\| \leqslant \|u\|^n$), 则前面的公式可写为形式 $\phi_z = e^{tu}\cdot z$.

e^{tu} 的计算可利用 u 的邓福德分解 $u = D + N$ 或者取 u 在某个基下的矩阵的若尔当形式来进行: 如果 $e_1, \ldots, e_m$ 是 V 的一组基, 在其下 u 的矩阵 A 具有若尔当形式, 则有 $A = D + N$, 其中 $D = \mathrm{Diag}(\lambda_1, \ldots, \lambda_m)$ 为对角矩阵, 而 N 是对角线为零的上三角矩阵, 且与 D 交换; 由于 D 和 N 交换, 故 $e^{tu} = e^{tD}e^{tN}$, 而 $e^{tD} = \mathrm{Diag}(e^{\lambda_1 t}, \ldots, e^{\lambda_m t})$, 又因为 $N^m = 0$, 有 $e^{tN} = \sum_{n=0}^{m-1} \frac{t^n N^n}{n!}$.

(iv) 设 I 是 $\mathbf{R}$ 的一个区间, 而 $f : V \times I \to V$ 满足关于 u 的利普希茨条件 (即如果 $J \subset I$ 是个紧区间, 则存在 $C(J)$ 使得 $\|f(u_1, t) - f(u_2, t)\| \leqslant C(J)\|u_1 - u_2\|$, 其中 $u_1, u_2 \in V, t \in J$ 任意). 按同样的证明得到微分方程 $u' = f(u, t)$ 在整个 I 上有唯一的解, 满足初始条件 $u(t_0) = u_0$, 其中 $u_0 \in V$ 任意. 如果我们去掉 "$f : V \times I \to V$ 对 u 满足利普希茨条件" 则此结论不成立: $u' = u^2$ 在 0 取 1 的解是 $t \mapsto \frac{1}{1-t}$ 在 $t = 1$ 突增, 不能扩张到整个 $\mathbf{R}$ 上.

4.2. 朗斯基行列式和常量变易法

定理 II.1.12 给了我们一个函数 $a : I \to \mathrm{GL}(V)$ 使得微分方程组 $\phi' = u \cdot \phi$ 的在 t_0 取值 z 的解 ϕ_z 为 $a \cdot z$.

命题 II.1.14. — (i) $a : I \to \mathrm{GL}(V)$ 满足微分方程 $a' = ua$.

(ii) a 的行列式 W(它是该微分方程组的朗斯基行列式) 满足微分方程 $W' = (\mathrm{Tr}(u))W$, 并对所有 $t \in I$ 有 $W(t) = \exp(\int_{t_0}^t \mathrm{Tr}(u(t))dt)$(刘维尔公式). [275]

证明 如果 $z \in V$, 则 $\phi_z = a \cdot z$, 从而 $\phi_z' = a' \cdot z$. 但由于另有 $\phi_z' = u \cdot \phi_z$, 故得到 $a' \cdot z = ua \cdot z$, $z \in V$, 因此 $a' = ua$. (i) 得证.

为了证明 (ii), 我们选取 V 的一组基 $e_1, \ldots, e_n$. 由于行列式是 n 重线性的, 故由 $\phi_{e_i}'(t) = u(t) \cdot \phi_{e_i}(t)$ 有

$$W'(t) = (\det_{e_1,\ldots,e_n}(\phi_{e_1}(t), \ldots, \phi_{e_n}(t))' = \sum_{i=1} \det_{e_1,\ldots,e_n}(\phi_{e_1}(t), \ldots, \phi_{e_i}'(t), \ldots, \phi_{e_n}(t)).$$

且由于

$$\text{(II.1.1)} \qquad \sum_{i=1}^n \det_{e_1,\ldots,e_n}(v_1, \ldots, u \cdot v_i, \ldots, v_n) = Tr(u) \det_{e_1,\ldots,e_n}(v_1, \ldots, v_n),$$

故得到了所要求的微分方程 $W' = (\mathrm{Tr}(u))W$, 它的满足在 t_0 取值为 1 的唯一的解为 $t \mapsto \exp(\int_{t_0}^t \mathrm{Tr}(u(t))dt)$. 得到了结论.(为了证明公式 (II.1.1), 我们注意到等式的两端都是 $(v_1, \ldots, v_n)$ 的 n 重交错线性形式, 从而只要证明在 V 的一组选好的基上相同即可; 就用基 $(e_1, \ldots, e_n)$, 并因为 $\det_{e_1,\ldots,e_n}(e_1, \ldots, u \cdot e_i, \ldots, e_n) = u_{i,i}$, 其中 u 在此基下的矩阵为 $(u_{i,j})$. 故得结果.) □

习题 II.1.15. — 证明 $\det(\exp A) = e^{\mathrm{Tr}(A)}$, 其中 $A \in \mathbf{M}_n(\mathbf{C})$.(先从 A 为三角矩阵做起.)

现在我们的兴趣在具有第二项的微分方程组[41]上, 就是说形如 $\phi' - u\cdot\phi = v$ 的方程, 其中 $v: I \to V$ 连续. 如果我们有一个该方程组的特解 ϕ_0, 那么 $\phi \mapsto \phi - \phi_0$ 诱导了具有第二项的方程组 $\phi' - u\cdot\phi = v$ 的解的集合与无第二项的方程组 $\phi' - u\cdot\phi = 0$ 的解的集合之间的一个双射. 解具有第二项的微分方程组等价于找一个特解与解一个无第二项的方程组.

进一步说, 如果我们已经知道了无第二项的方程组的解, 那么我们则可以应用常量变易的方法来求具有第二项的方程组的一个特解. 无第二项的方程组的解法给了我们微分方程组 $a' = ua$ 的一个解 $a : I \to \mathrm{GL}(V)$, 以及方程组 $\phi' = u\cdot\phi$ 的解 $t \mapsto a(t)\cdot z$, $z \in V$ 任意. 常量变易法是找 $\phi' - u\cdot\phi = v$ 的一个形如 $\phi(t) = a(t)\cdot z(t)$ 的解. 于是有 $\phi'(t) = a'(t)\cdot z(t) + a(t)\cdot z'(t)$, 从而 $a'(t)\cdot z(t) + a(t)\cdot z'(t) - u(t)a(t)\cdot z(t) = v(t)$; 由于 $a' = ua$, 故此方程简化为 $z' = a^{-1}\cdot v$, 用简单的积分即可解此方程.

4.3. 高阶微分方程 [276]

推论 II.1.16. — 设 $I \subset \mathbf{R}$ 为开区间. 如果 $a_0, \ldots, a_{n-1}$ 是从 I 到 $\mathbf{K}$ 的连续函数, 微分方程 $\phi^{(n)} = a_{n-1}\phi^{(n-1)} + \cdots + a_0\phi$ 在 I 上的解的集合 $\mathscr{L}$ 是一个 n 维的向量空间, 并且对每个 $t \in I$, 映射 $\phi \mapsto (\phi(t), \ldots, \phi^{(n-1)}(t))$ 是 $\mathscr{L}$ 到 $\mathbf{K}$ 的一个同构. 换而言之,

- 如果 $t_0 \in I$, 而 $z = (z_0, \ldots, z_{n-1}) \in \mathbf{K}^n$, 则在整个 I 上存在微分方程 $\phi^{(n)} = a_{n-1}\phi^{(n-1)} + \cdots + a_0\phi$ 唯一的解 ϕ_z, 使得 $\phi_z^{(i)}(t_0) = z_i, 0 \leqslant i \leqslant n-1$;
- 如果 $i \in I$, 则存在 $A(t) \in \mathbf{GL}_n(\mathbf{K})$ 使得 ${}^t(\phi_z(t), \phi_z'(t), \ldots, \phi_z^{(n-1)}(t)) = A(t)\,{}^t z$.

证明 设

$$U = \begin{pmatrix} 0 & 1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & 1 \\ a_0 & \ldots & a_{n-2} & a_{n-1} \end{pmatrix}.$$

如果 $\Phi = {}^t(\phi_0, \ldots, \phi_{n-1})$ 是微分方程组 $\Phi' = U\Phi$ 在 I 上的一个解, 则 $\phi_0, \ldots, \phi_{n-1}$ 属于 $\mathscr{C}^1$ 类, 且 $\phi_0' = \phi_1, \ldots, \phi_{n-2}' = \phi_{n-1}$ 而 $\phi_{n-1}' = a_0\phi_0 + \cdots + a_{n-1}\phi_{n-1}$. 由此推出 $\phi = \phi_0$ 属于 $\mathscr{C}^n$, 而对 $0 \leqslant i \leqslant n-1$, $\phi_i = \phi^{(i)}$, 并且 ϕ 满足微分方程 $\phi^{(n)} = a_{n-1}\phi^{(n-1)} + \cdots + a_0\phi$. 反之, 如果 ϕ 是这个方程的一个解, 则 $\Phi = {}^t(\phi, \ldots, \phi^{(n-1)})$ 便是微分方程组 $\Phi' = U\Phi$ 的解. 换而言之 $\Phi \mapsto \phi_0$ 是从 $\Phi' = U\Phi$ 的解空间到 $\phi^{(n)} = a_{n-1}\phi^{(n-1)} + \cdots + a_0\phi$ 的解空间的一个同构. 这样这个推论便是定理 II.1.12 的简单转换. □

注记 II.1.17. — (i) 具有第二项的方程 $\phi^{(n)} - a_{n-1}(t)\phi^{(n-1)} + \cdots - a_0(t)\phi = b(t)$ 可对推论 II.1.16 中的相伴形式应用常量变易法解.

(ii) 如果微分方程是常系数的, 这些解是矩阵 e^{tU} 的系数, 其中 U 是上面的那个矩阵 (由于 a_i 为常数, 故它与 t 无关). 如果 $\lambda_1, \ldots, \lambda_r$ 是 U 的特征值, 且 λ_i 的重数

[41] 即我们通常称为的 “非齐次方程组”, 而 “无第二项的方程组” 便是 “齐次方程组” 了.

为 d_i, 则对每个 λ_i 只有一个若尔当块 J_i(d_i 阶)(由习题 10.4 以及如下事实得到: 如果 $P \in K[X]$, $A \in \mathbf{M}_n(K)$, 则 $P({}^tA) = {}^t(P(A))$, 故一个矩阵和它的转置具有相同的极小多项式). 然而 $\exp(tJ_i)$ 的系数具有形式 $e^{\lambda_i t}P_i(t)$, 其中 $P_i \in \mathbf{C}[X]$ 的次数 $\leqslant d_i - 1$. 由此知 $t \mapsto e^{\lambda_i t}t^j$, $1 \leqslant i \leqslant r$, $0 \leqslant j \leqslant d_i - 1$ 构成了这个微分方程解空间的一组基. 例如, 如果这些 a_i 为 0, 则我们又重新得到了: n 阶导数恒等于零的 ϕ 的集合是次数 $\leqslant n-1$ 的多项式的空间.

[277] 5. 赋范向量空间的完备化

最标准的构造巴拿赫空间的方法是从赋范向量空间出发去做完备化[(6)]. 请回到小词典的 14.3 小节的那些处理度量空间的完备化的内容. 按通常的方式, 我们给出如下结果.

命题 II.1.18. — (i) 如果 $(E, \| \ \|)$ 是一个赋范向量空间, 那么 E 的完备化 $\widehat{E}$ (按与 $\| \ \|$ 相伴的距离) 是一个向量空间. 另外, $\| \ \|$ 被连续地延拓为 $\widehat{E}$ 上的一个范数, 而 $(\widehat{E}, \| \ \|)$ 是一个巴拿赫空间.

(ii) 如果 F 是一个巴拿赫空间, 且 $u : E \to F$ 是一个连续的线性映射, 则 u 有唯一的到 $\widehat{E}$ 上的连续扩张, 而此扩张是线性的.

证明　反复使用 14.3 小节的结果便得到 (i), 这只是个小习题. 例如要证明加法 $s : E \times E \to E$ 可连续地扩张为一个加法 $s : \widehat{E} \times \widehat{E} \to \widehat{E}$, 我们可赋予 $E \times E$ 范数为 $\|(x, y)\| = \sup(\|x\|, \|y\|)$. 于是 $s : E \times E \to E \subset \widehat{E}$ 是比率 2 的利普希茨映射, 因而可连续地扩张到 $\widehat{E} \times \widehat{E}$ 上.

至于 (ii), 见小词典的 17.2 小节. □

例题 II.1.19. — 设 Ω 是 $\mathbf{R}^m$ 中的一个开集.

(i) 在 §III.2 的 1 小节中定义的 $L^1(\Omega)$ 是一个巴拿赫空间, 在其中 $\mathscr{C}_c(\Omega)$ 稠密; 我们也可定义它为 $\mathscr{C}_c(\Omega)$ 对于范数 $\| \ \|_1 : \|\phi\|_1 = \int_\Omega |\phi(x)|dx$ 的完备化.

(ii) 同样, 在 §III.2 的 2 小节中定义的 $L^2(\Omega)$ 也可定义为 $\mathscr{C}_c(\Omega)$ 对于范数 $\| \ \|_2 : \|\phi\|_2 = (\int_\Omega |\phi(x)|^2 dx)^{1/2}$ 的完备化.

(iii) 如果 $k \geqslant 1$, 定义索伯列夫空间 $H^k(\mathbf{R}^m)$ 为 $\mathbf{R}^m$ 上的 $\mathscr{C}^k$ 类的在一个紧集外为零的函数的空间 $\mathscr{C}_c^k(\mathbf{R}^m)$, 其范数 $\| \ \|_{H^k}$ 为:

$$\|\phi\|_{H^k} = (\sum_{|\boldsymbol{\ell}| \leqslant k} (\|\partial^{\boldsymbol{\ell}}\phi\|_2)^2)^{1/2} = (\sum_{|\boldsymbol{\ell}| \leqslant k} \int_{\mathbf{R}^m} |\partial^{\boldsymbol{\ell}}\phi(x)|^2 dx)^{1/2},$$

[(6)]这对很多问题是非常有用的, 因为我们得到了一个在其中做分析变得更加容易的空间; 特别地, 在一个完备的空间中证明存在性的结果要容易得多. 显然, 问题是在完备化后要恢复到原来的情形是很困难的. 譬如, 不可能证明两个实数相等 ($\mathbf{R}$ 由 $\mathbf{Q}$ 的完备化得到) 除非我们进一步知道它们的差是一个整数 (容许乘以一个显式表达的实数). 同样, 在一个索伯列夫空间 H^k 中更加容易证明微分方程的存在性, 但是如果我们感兴趣的是 $\mathscr{C}^k$ 类的解的存在性, 则还需要补充的工作去证明这些得到的解是这样的.

其中如果 $\boldsymbol{\ell}=(\ell_1,\ldots,\ell_m)\in\mathbf{N}^m$, 则令 $|\boldsymbol{\ell}|=\sum_{j=1}^m \ell_j$, 并以 $\partial^{\boldsymbol{\ell}}$ 代表微分算子 [278]

$$\partial^{\boldsymbol{\ell}}=(\frac{\partial}{\partial x_1})^{\ell_1}\cdots(\frac{\partial}{\partial x_m})^{\ell_m}.$$

如果在 $\mathscr{C}_c^k(\mathbf{R}^m)$ 上赋予范数 $\|\ \|_{H^k}$, 并在 $\mathscr{C}_c^{k-|\boldsymbol{\ell}|}(\mathbf{R}^m)$ 上赋予 $\|\ \|_{H^{k-|\boldsymbol{\ell}|}}$, 则按定义, 如果 $\boldsymbol{\ell}=(\ell_1,\ldots,\ell_m)\in\mathbf{N}^m$ 满足 $|\boldsymbol{\ell}|\leqslant k$, 那么线性映射

$$\partial^{\boldsymbol{\ell}}=(\frac{\partial}{\partial x_1})^{\ell_1}\cdots(\frac{\partial}{\partial x_m})^{\ell_m}:\mathscr{C}_c(\mathbf{R}^m)\to\mathscr{C}_c^{k-|\boldsymbol{\ell}|}(\mathbf{R}^m)$$

是连续的 (甚至是 1-利普希茨的). 因此可连续地扩张为从 $H^k(\mathbf{R}^m)$ 到 $H^{k-|\boldsymbol{\ell}|}(\mathbf{R}^m)$ 的一个线性映射, 并仍记以 $\partial^{\boldsymbol{\ell}}$.

命题 II.1.20. — 如果 $k\in\mathbf{N}$, 而 $\boldsymbol{\ell}\in\mathbf{N}$ 满足 $|\boldsymbol{\ell}|\leqslant k$, 又如果 $\phi\in\mathscr{C}_c^k(\mathbf{R}^m)$, $f\in H^k(\mathbf{R}^m)$, 则[7]

$$\int_{\mathbf{R}^m}(\partial^{\boldsymbol{\ell}}\phi)f=(-1)^{|\boldsymbol{\ell}|}\int_{\mathbf{R}^m}(\partial^{\boldsymbol{\ell}}f)\phi.$$

证明 由于 $\partial^{\boldsymbol{\ell}}\phi, f, \partial^{\boldsymbol{\ell}}f$ 和 ϕ 都是平方可和的, 故上式两端都有定义. 由此得到

$$f\mapsto L_\phi(f)=\int_{\mathbf{R}^m}(\partial^{\boldsymbol{\ell}}\phi)f-(-1)^{|\boldsymbol{\ell}|}\int_{\mathbf{R}^m}(\partial^{\boldsymbol{\ell}}f)\phi$$

是 $H^k(\mathbf{R}^m)$ 上的线性形式, 而且由于

$$|L_\phi(f)|\leqslant\|f\|_2\|\partial^{\boldsymbol{\ell}}\phi\|_2+\|\partial^{\boldsymbol{\ell}}f\|_2\|\phi\|_2\leqslant(\|\partial^{\boldsymbol{\ell}}\phi\|_2+\|\phi\|_2)\|f\|_{H^k},$$

故此线性形式连续. 另外, 分部积分表明, 当 $f\in\mathscr{C}_c^k(\mathbf{R}^m)$ 时 $L_\phi(f)=0$, 并因为 $\mathscr{C}_c^k(\mathbf{R}^m)$ 在 $H^k(\mathbf{R}^m)$ 中稠密, 这表明 L_ϕ 在 $H^k(\mathbf{R})$ 上恒等于 0. 得证. □

6. 巴拿赫空间之间的连续线性映射

定理 II.1.21. — (巴拿赫 - 施泰豪斯, 1927) 设 E 为巴拿赫空间, F 是一个赋范向量空间, 而 $(u_n)_{n\in\mathbf{N}}$ 是从 E 到 F 的一个连续的线性映射的序列. 于是下面两个之一成立:

- 或者序列 $(\|u_n\|)_{n\in\mathbf{N}}$ 有界[8], 从而 $u_n(x)$ 对所有的 $x\in E$ 有界,
- 或者 $\{x\in E,\sup_{n\in\mathbf{N}}\|u_n(x)\|_F=+\infty\}$ 在 E 中稠密.

证明 我们要证明, 如果 $(\|u_n\|)_{n\in\mathbf{N}}$ 不是有界的, 并定义 $\varphi:E\to\mathbf{R}_+\cup\{+\infty\}$ 为 $\varphi(x)=\sup_{n\in\mathbf{N}}\|u_n(x)\|_F$, 则 $\{x\in E,\varphi(x)=+\infty\}$ 稠密. 为此, 对 $N\in\mathbf{N}$, 考虑集合 $U_N=\{x\in E,\varphi(x)>N\}$. 于是我们有 $U_N=\cup_{n\in\mathbf{N}}\{x\in E,\|u_n(x)\|_F>N\}$, 并且由于 u_n 连续, U_N 便是开集的并, 从而也是开集. 如果 U_N 不稠密, 则存 [279]

---

[7] 换而言之, $\partial^{\boldsymbol{\ell}}f$ 是在广义函数的意义下的 $\boldsymbol{\ell}$ 阶导数 (即所谓的广义导数 —— 译者注).

[8] $\|u_n\|$ 是 u_n 算子范数. 回忆一下它的定义: $\|u_n\|=\sup_{x\neq0}\|x\|_E^{-1}\|u_n(x)\|_F$, 参看 §11 的 17 小节.

在 $x_0 \in E$ 和 $r > 0$ 使得 $\|u_n(x+x_0)\|_F \leqslant N$ 对于满足 $\|x\|_E < r$ 的 $x \in E$ 和 $n \in \mathbf{N}$ 都成立. 于是对于满足 $\|x\| < r$ 的所有 $x \in E$ 和任意的 $n \in \mathbf{N}$ 有 $\|u_n(x)\|_F = \|u_n(x+x_0) - u_n(x_0)\|_F \leqslant 2N$. 换而言之, 对于任意的 $n \in \mathbf{N}$ 我们有 $\|u_n\| \leqslant \frac{2N}{r}$, 与假设矛盾. 于是对于任意的 $N \in \mathbf{N}$, U_N 是个开稠集, 并由于 $\{x \in E, \varphi(x) = +\infty\} = \cap_{N\in\mathbf{N}} U_N$, 根据贝尔引理 (小词典的 14.2 小节) 它在 E 中稠密. 得证. □

注记 II.1.22. — 由这个证明知道, 如果 $\|u_n\|$ 不是有界的, 则 $\{x \in E, \sup_{n\in\mathbf{N}} \|u_n(x)\|_F = +\infty\}$ 是可数个开稠集的交. 称可数个开集的交集是一个 G_δ, 那么由贝尔引理知, 一个在巴拿赫空间中稠密的 G_δ 集是不可数的 (参看小词典的习题 14.3).

巴拿赫 – 施泰豪斯定理有如下一个非常有用的推论, 它在考虑连续函数的简单极限时会带来出人意料的结果[9].

推论 II.1.23. — 如果 E 为巴拿赫空间, 且 F 为赋范向量空间, 则从 E 到 F 的连续线性映射的简单极限是 E 到 F 的一个连续线性映射.

证明　设 $(u_n)_{n\in\mathbf{N}}$ 是从 E 到 F 的一个连续线性映射的序列使得对任意的 $x \in E$, 级数 $(u_n(x))_{n\in\mathbf{N}}$ 收敛到极限 $u(x) \in F$. 如果 $x \in E$ 和 $\lambda \in \mathbf{K}$, 则有 $u(\lambda x) = \lim_{n\to+\infty} u_n(\lambda x) = \lim_{n\to+\infty} \lambda u_n(x) = \lambda \lim_{n\to+\infty} u_n(x) = \lambda u(x)$, 同样, 对于任意的 $x, y \in E$ 有 $u(x+y) = u(x) + u(y)$, 这些证明了 u 是线性的. 现在, 按照巴拿赫 – 施泰豪斯定理, 对于任意的 $x \in E$ 序列 $(u_n(x))_{n\in\mathbf{N}}$ 有极限说明存在 $M \in \mathbf{R}_+$ 使得当 $n \in \mathbf{N}$ 时 $\|u_n\| \leqslant M$. 因此 $\|u_n(x)\|_F \leqslant M \cdot \|x\|_E$, 其中 $x \in E$ 和 $n \in \mathbf{N}$. 过渡到极限则对任意的 $x \in E$ 得到 $\|u(x)\|_F \leqslant M \cdot \|x\|_E$, 从而 u 连续. 得到结论. □

定理 II.1.24. — (开映像定理, 巴拿赫 (1929)) 如果 E 和 F 是两个巴拿赫空间, 且 $u : E \to F$ 是一个满的连续线性映射, 则存在 $\rho > 0$ 使得 $u(B_E(0, 1^-))$ 包含了 $B_F(0, \rho^-)$.

证明　如果 $n \in \mathbf{N}$, 令 A_n 为 $u(B_E(0, n^-))$ 在 F 中的闭包. 由于 E 是这些 $B_E(0, n^-)$, $n \in \mathbf{N}$ 的并, 而且 u 是满的, 故有 $\cup_{n\in\mathbf{N}} A_n = F$. 贝尔引理表明存在 [280] n 使得 A_n 的内核非空. 这等于说存在 $x_0 \in B_E(0, n^-)$ 和 $r > 0$, 使得当 $\|y\|_F < r$ 时, 对于任意的 $\varepsilon > 0$, 存在 $x \in B_E(0, n^-)$ 满足 $\|u(x) - (u(x_0) + y)\|_F < \varepsilon$. 因为 $x - x_0 \in B_E(0, 2n^-)$, 如有必要可作比率为 $\frac{1}{4n}$ 的位似变换, 则可看出我们已经证明了后面的结果, 即存在 $\rho > 0$(实际 $\rho = \frac{1}{4n}$) 使得对于任意的 $y \in B_F(0, \rho^-)$ 和任意的 $\varepsilon > 0$, 存在 $x \in B_E(0, (\frac{1}{2})^-)$ 满足 $\|y - u(x)\|_F < \varepsilon$.

这还不是我们要的结果, 但却差不多了. 如果 $y \in B_F(0, \rho^-)$, 我们则可应用前面所证归纳地构造一个由 $B_E(0, (\frac{1}{2})^-)$ 中的元构成的序列 $(x_m)_{m\in\mathbf{N}}$, 以及一个

[9] 尽管柯西在他的《分析教程》(Cours d'analyse) 成功地 "证明" 了连续函数的简单极限仍是连续的, 但从今天来看, 我们知道他什么也没有证明. 贝尔 (1904) 证明了一个函数 $f : R^n \to \mathbf{R}$ 是连续函数的简单极限当且仅当 f 在每个非空闭集上的限制至少在其中一个点连续. 这就是他的著名引理所给出的情形.

由 $B_F(0,\rho^-)$ 中的元构成的序列 $(y_m)_{m\in\mathbf{N}}$, 满足

$$y_0 = y,\ \|y_m - u(x_m)\|_F < \frac{\rho}{2},\ y_{m+1} = 2(y_m - u(x_m)).$$

因此有 $y = u(x_0)+2^{-1}u(x_1)+\cdots+2^{-m}u(x_m)+2^{-m-1}y_{m+1}$, 而由于序列 $\sum_{m=0}^{+\infty} 2^{-m}x_m$ 在 E 中收敛于 $B_E(0,1^-)$ 中的一个元 x, 取极限便得到了 $y = u(x)$. 这证明了 $B_F(0,\rho^-) \subset u(B_E(0,1^-))$. 即为所证. □

注记 II.1.25. — 如果 $x\in E, r>0$, 则 $B_E(x,r^-) = x+rB_E(0,1^-)$, 因此 $u(B_E(x,r^-)) = u(x) + ru(B_E(0,1^-))$. 上面的定理因而证明了, 如果 u 为满射, 则 $u(B_E(x,r^-))$ 包含了 $u(x)$ 的一个开邻域. 由此得知, 如果 U 是 E 的一个开集, 则对任意的 $x \in U$, $u(U)$ 是 $u(x)$ 的一个开邻域, 或者说 $u(U)$ 是一个开集. 于是上面的定理可以重新叙述为"在两个巴拿赫空间之间的一个满的连续线性映射下, 开集的像仍为开集"; 这就解释了它的名称的由来.

推论 II.1.26. — 如果 E 和 F 为两个巴拿赫空间, 而 $u: E \to F$ 是一个连续的线性双射, 则 $u^{-1}: F \to E$ 也连续.

证明 如果 U 是 E 的一个开集, 则由上面的注记知 $(u^{-1})^{-1}(U) = u(U)$ 是个开集. 从而得到结论. □

习题 II.1.27. — (闭图像定理) 设 E 和 F 为两个巴拿赫空间, 而 $u: E \to F$ 为线性映射. 设 $G \subset E \times F$ 是 u 的图像 (即集合 $\{(x,u(x)), x \in E\}$).

(i) 证明赋予了范数 $\|(x,y)\| = \sup(\|x\|_E, \|y\|_F)$ 的 $E \times F$ 是一个巴拿赫空间, 且两个投射 $p_E: E \times F \to E$ 和 $p_F: E \times F \to F$ 均连续.

(ii) 证明 G 是 $E \times F$ 的一个向量子空间, 并且如果 G 在 $E \times F$ 是个闭集, 则 u 连续. (注意 p_E 和 p_F 在 G 上的限制.)

(iii) 构造 $f: \mathbf{R} \to \mathbf{R}$, 使它不连续但其图像为闭集.

7. 巴拿赫空间的对偶

如果 E 是个赋范线性空间, 以 E^* 记其对偶; 就是说, E 上的连续线性形式的集合. 如果 $\Lambda: E \to \mathbf{K}$ 是一个连续的线性形式, 我们曾定义过一个范数 $\|\Lambda\|$ 为使得 [281] $|\Lambda(x)| \leqslant C\|x\|, \forall\, x \in E$ 的那些 $C \in \mathbf{R}_+$ 的下确界.

定理 II.1.28. — 如果 E 是一个赋范向量空间, 则 $(E^*, \|\ \|)$ 是一个巴拿赫空间.

证明 在小词典的 17.3 小节中已经证明过 $\|\ \|$ 是一个向量空间的范数. 现设 Λ_n 是 E^* 中的一个使得 $\sum_{n\in\mathbf{N}} \|\Lambda_n\| = C < +\infty$ 的序列. 如果 $x \in E$, 级数 $\sum_{n\in\mathbf{N}} \Lambda_n(x)$ 绝对收敛, 且存在 $\Lambda(x)$ 使得级数 $|\Lambda(x)| \leqslant \sum_{n\in\mathbf{N}} |\Lambda_n(x)| \leqslant C\|x\|$. 另外, 由于 $x \mapsto \Lambda x$ 是线性的, 上面的囿于上的强函数关系表明 $x \mapsto \Lambda(x)$ 也是连续的, 由此推出 $\Lambda \in E^*$, 并且 $\sum_{n\in\mathbf{N}} \Lambda_n = \Lambda$. 证完. □

定理 II.1.29. — (哈恩 – 巴拿赫, 1927) 如果 E 是一个赋范向量空间, 而 F 是 E 的一个向量子空间, 并且 f 是 F 上的一个连续线性形式, 则存在 $\Lambda \in E^*$, 使得它在 F 上的限制为 f, 并满足 $\|\Lambda\| = \|f\|$.

我们不打算给出哈恩 – 巴拿赫定理的证明 (证明需要用到选择公理), 但它有一些有用的推论, 包括 $E^* \neq 0$. 在下面的习题中我们找到了另外的办法.

习题 II.1.30. — 证明 F 在 E 中的闭包 $\overline{F}$ 是在 F 上为零的 E 上的连续线性形式的核的交.

习题 II.1.31. — (i) 证明, 如果 $x_0 \in E$, 则存在 $\Lambda \in E^*$ 满足 $\|\Lambda\| = 1$ 和 $|\Lambda(x_0)| = \|x_0\|$.

(ii) 证明 E^* 分离点 (如果 $x \neq y$, 则存在 $\Lambda \in E^*$ 使得 $\Lambda(x) \neq \Lambda(y)$).

(iii) 证明映射 $\Lambda \mapsto \Lambda(x)$ 是 E^* 上的一个连续线性形式, 并诱导了从 E 到 $(E^*)^*$ 的一个等距映射. (如果这个等距映射是个双射, 从而 E 恒等于它的对偶的对偶, 则称巴拿赫空间 E 是自反的; 一般地, $(E^*)^*$ 可能会比 E 大很多, 但根据里斯定理 (定理 II.2.12) 希尔伯特空间是自反的.)

II.2. 希尔伯特空间

希尔伯特空间是一个具有特别好的数学性质的巴拿赫空间: 希尔伯特基的存在性证明我们在实践中遇到的那些空间都是同构的, 而正交投射的存在性让我们经常归结到有限维的情形. 构造非常合理的大自然的正是这些空间, 它们自然地存在于许多物理问题中 (譬如在量子力学中).

1. 希尔伯特空间

希尔伯特空间是一个完备的准希尔伯特空间 (参看小词典的 §18); 因而是巴拿赫空间的特殊情形.

例题 II.2.1. — (i) 具有标量积的有限维空间是希尔伯特空间.

(ii) 如果 E 是一个准希尔伯特空间, 它的完备化 $\widehat{E}$ 是一个希尔伯特空间 (标量积由连续性延拓). [282]

(iii) ℓ^2, 或更一般的 $\ell^2(I)$, I 可数, 是希尔伯特空间.

(iv) 如果 Ω 是 $\mathbf{R}^n$ 上的一个开集, 则 $L^2(\Omega)$ 是希尔伯特空间.

(v) $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ 在范数 $\|\ \|_2 : \|f\|_2 = \int_0^1 |f(t)|^2 dt$ 下的完备化 $L^2(\mathbf{R}/\mathbf{Z})$ 是希尔伯特空间 (标量积为 $\langle f, g\rangle = \int_0^1 \overline{f(t)} g(t) dt$).

(vi) 索伯列夫空间 $H^k(\mathbf{R}^m)$ 是希尔伯特空间.

1.1. 希尔伯特基

设 E 是一个无限维的可分的[10]希尔伯特空间. E 的一个希尔伯特基[11] 是 E 的一族可数的法正交的元 $(e_i)_{i\in I}$, 使得由这些 $e_i, i \in I$ 生成的 E 的子空间在 E 中稠密.

例题 II.2.2. — (i) 如果 I 是一个可数集, 则 $\ell^2(I)$ 具有一个自然的希尔伯特基, 即那些 $e_i, i \in I$ 构成, 其中的 e_i 是在 i 为 1 而在其他为 0 的序列.

(ii) $e^{2i\pi nt}, n \in \mathbf{Z}$ 构成 $L^2(\mathbf{R}/\mathbf{Z})$ 的一个希尔伯特基.

证明 (i) 这些 e_i 是一个法正交族直接可得. 现在, 如果 $x = (x_i)_{i\in I} \in \ell^2(I)$, 且若 $J \subset I$ 为有限集, 则 $\|x - \sum_{j\in J} x_j e_j\|_2^2 = \sum_{i\in I-J} |x_j|^2$. 由于 $\sum_{j\in I} |x_i|^2 < +\infty$, 于是可以使得当 J 增大时 $\|x - \sum_{j\in J} x_j e_j\|_2$ 也任意地小, 这证明了由这些 e_i, $i \in I$ 生成的子空间在 $\ell^2(I)$ 中稠密. 由此推出 (i).

(ii) 直接计算可证明这些 $e^{2i\pi nt}$ 是一个法正交族; 它们生成的空间是三角多项式的空间. 如果 $f \in L^2(\mathbf{R}/\mathbf{Z})$, 且 $\varepsilon > 0$, 则由 $L^2(\mathbf{R}/Z)$ 的定义知存在 $\mathbf{R}/\mathbf{Z}$ 上的一个连续函数 g 满足 $\|f - g\|_2 < \frac{\varepsilon}{2}$. 另外, 根据斯通 – 魏尔斯特拉斯定理 (参看习题 II.1.10 的 (iii)), 三角多项式的空间在 $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ 中稠密; 因此存在三角多项式 P 使得 $\|P - g\|_\infty < \frac{\varepsilon}{2}$. 由于如果 $h \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$ 便有 $\|h\|_2 \leqslant \|h\|_\infty$, 故 $\|f - P\|_2 < \varepsilon$, 这证明了 $L^2(\mathbf{R}/\mathbf{Z})$ 中的每个开球都包含了一个三角多项式, 因此有 $e^{2i\pi nt}$, $n \in \mathbf{N}$ 在 $L^2(\mathbf{R}/\mathbf{Z})$ 中稠密. 得证. □

命题 II.2.3. — 一个可分的希尔伯特空间具有希尔伯特基.

证明 设 E 是一个可分的希尔伯特空间, $A \subset E$ 是一个稠密的可数子集. 为了从 A 构造出一个希尔伯特基, 我们将 A 中的元编号, 并消去那些在由前面的元生成的向量空间中的元, 这给出了由 A 生成的向量空间 E' 的基 $(b_i)_{i\in I}$, $I \subset \mathbf{N}$. 最后, 应用斯密特法正交过程构造出 E 中的元构成的法正交族, 它们生成了 E'; 因为 E' 包含了 A, 故在 E 中稠密, 于是这个族是 E 的希尔伯特基. □ [283]

1.2. 在一个闭子空间上的正交投射

引理 II.2.4. — 设 E 为希尔伯特空间, 而 $(e_i)_{i\in I}$ 是 E 中的元构成的可数法正交族.

(i) 如果 $(x_i)_{i\in I}$ 是 $\mathbf{C}$ 中的一族元, 则级数 $\sum_{i\in I} x_i e_i$ 可和当且仅当 $(x_i)_{i\in I} \in \ell^2(I)$.

(ii) 如果 $(x_i)_{i\in I} \in \ell^2(I)$, 且 $x \in E$ 是级数 $\sum_{i\in I} x_i e_i$ 的和, 则对于每个 $i \in I$ 有 $\langle e_i, x\rangle = x_i$ 和 $\|x\|^2 = \sum_{i\in I} |x_i|^2$.

证明 由族 $(e_i)_{i\in I}$ 的法正交性, 对于每个有限的 $J \subset I$ 有 $\|\sum_{i\in J} x_i e_i\| = (\sum_{i\in J} |x_i|^2)^{1/2}$. $\sum_{i\in J} x_i e_i$ 的可和性于是等价于条件 $\sum_{i\in I} |x_i|^2 < +\infty$. 这就得到了 (i).

[10] 随后的理论也可推广到不可分的希尔伯特空间. 但在实际中极少遇到. 唯一的差别在于当 E 不是可分的时候, 希尔伯特基的基数是不可数的.

[11] 一个希尔伯特基也经常被称作一个法正交基. 注意如下事实: 一个希尔伯特基, 一般来说, 不是在代数意义下的基. 更准确地说, 希尔伯特基是代数基当且仅当它是有限维的, 但这在泛函分析中是罕见的.

如果 I 有限, 则 (ii) 显然. 故不妨设 $I=\mathbf{N}$. 于是 x 是通项为 $y_n=\sum_{j=0}^n x_je_j$ 的序列的极限, 因为对所有 $n\geqslant i$ 有 $\langle e_i,y_n\rangle=x_i$ 以及 $\|y_n\|^2=\sum_{j=0}^n|x_j|^2$, 再利用范数和标量积的连续性, 经取极限便得到了 (ii). □

命题 II.2.5. — 设 F 是 E 的一个闭子向量空间, 其中 F 具有一个希尔伯特基 $(e_i)_{i\in I}$.

(i) 如果 $x\in E$, 则 $(\langle e_i,x\rangle)_{i\in I}\in\ell^2(I)$.

(ii) 级数 $\sum_{i\in I}\langle e_i,x\rangle e_i$ 可和; 它的和 $p_F(x)$ 属于 F, 并有恒等式 $\|p_F(x)\|^2=\sum_{i\in I}|\langle e_i,x\rangle|^2$.

(iii) $p_F:E\to F$ 是一个投射, 并且 $p_F(x)$ 是 F 中使得 $x-p_F(x)$ 正交于整个 F 的唯一的元. 另外, p_F 还是 1-利普希茨的.

证明　如果 F 为有限维的, 这个结果已在小词典的 18.2 小节中证明了. 现设 $I=\mathbf{N}$. 以 F_i 记由 e_j, $j\leqslant i$ 生成的 E 的向量子空间. 于是 $y_i=\sum_{j=0}^i\langle e_j,x\rangle e_j$ 是 x 在 F_j 中的正交投射. 特别地, $\sum_{j=0}^i|\langle e_i,x\rangle|^2=\|y_i\|^2\leqslant\|x\|^2$, 其中 $i\in\mathbf{N}$. 由此推出 $(\langle e_i,x\rangle)_{i\in\mathbf{N}}$ 属于 ℓ^2, (i) 得证.

(ii) 是引理 II.2.4 的直接推论, 由它也推出了 $x-p_F(x)$ 与所有的 e_i 正交, 从而由线性性和稠密性, 它与整个 F 正交. 剩下的 (iii) 来自到子空间 (不必为闭空间, 参看小词典的 18.2 小节) 的正交投射的唯一性. 证毕. □

[284] **定理 II.2.6.** — 如果 $(e_i)_{i\in I}$ 是 E 的一个希尔伯特基, 则映射 $x\mapsto(\langle e_i,x\rangle)_{i\in I}$ 诱导了从 E 到 $\ell^2(I)$ 的一个等距映射[12]. 换而言之,

(a) 如果 $x\in E$, 则 $(\langle e_i,x\rangle)_{i\in I}\in\ell^2(I)$ 和 $\sum_{i\in I}|\langle e_i,x\rangle|^2=\|x\|^2$ (贝塞尔 – 帕塞瓦尔 (Bessel-Parseval) 恒等式);

(b) 如果 $(x_i)_{i\in I}\in\ell^2(I)$, 则 $\sum_{i\in I}x_ie_i$ 在 E 中收敛, 且其和 x 对于每个 $i\in I$ 满足 $\langle e_i,x\rangle=x_i$.

证明　首先证明 "换而言之": (a) 可以重新叙述为 $x\mapsto(\langle e_i,x\rangle)_{i\in I}$ 是从 E 到 $\ell^2(I)$ 的一个子空间的等距映射, 而 (b) 则证明 $\ell^2(I)$ 是在 $x\mapsto(\langle e_i,x\rangle)_{i\in I}$ 的像中. 现在, (a) 由命题 II.2.5 的 (i) 和 (ii) 得到, 只要在其中用 $F=E$ 即可. 而 (b) 由 II.2.4 得到. □

如果我们将定理 II.2.6 特别用在由 $e^{2i\pi nt}$ 构成的 $L^2(\mathbf{R}/\mathbf{Z})$ 的希尔伯特基上, 则得到以下的结果.

推论 II.2.7. — 如果 $f\in L^2(\mathbf{R}/\mathbf{Z})$, 并令 $c_n(f)$ 为第 n 个傅里叶系数:

$$c_n(f)=\langle e^{2i\pi nt},f\rangle=\int_{\mathbf{R}/\mathbf{Z}}f(t)e^{-2i\pi nt}dt=\int_0^1 f(t)e^{-2i\pi nt}dt.$$

---

[12] ℓ^2 的一个无限维的闭子空间是一个可分的希尔伯特空间, 从而, 根据此定理, 同构于 ℓ^2. T. Gowers 得到 1998 年的菲尔兹奖很大程度上在于证明了上述性质特征地刻画了 ℓ^2: 一个可分的巴拿赫空间, 如果同构于它的每个无限维的闭子空间, 则它同构于 ℓ^2.

于是在 $L^2(\mathbf{R}/\mathbf{Z})$ 中[13] $f=\sum_{n\in\mathbf{Z}} c_n(f)e^{2i\pi nt}$, $\sum_{n\in\mathbf{Z}} |c_n(f)|^2=(\|f\|_2)^2=\int_0^1 |f(t)|^2dt$ (贝塞尔 – 帕塞瓦尔).

推论 II.2.8. — (完全性判别法) 如果 $(e_i)_{i\in I}$ 是 E 中元的一个可数的法正交族, 则以下条件等价:

(i) $(e_i)_{i\in I}$ 是 E 的希尔伯特基.

(ii) 与每个 e_i 都正交的 $x\in E$ 的集合为 $\{0\}$.

证明 (i)⇒(ii) 是定理 II.2.6 的 (a) 的直接结果. 为了证明 (ii)⇒(i), 引进由这些 e_i 生成的空间在 E 中的闭包 F. 于是 $(e_i)_{i\in I}$ 是 F 的一个希尔伯特基, 而条件 (ii) 表明, 对于每个 $x\in E$ 有 $p_F(x)=x$, 从而 $F=E$. 得证. □

2. 投射到一个凸集上的定理

回忆, 如果 E 是 $\mathbf{K}$ 上的一个向量空间, 称 E 的一个子集 C 为凸的是说对于任意的 $x,y\in C$, C 包含线段 $[x,y]$. 特别地, 如果 C 为凸的, 且如果 $x,y\in C$, 则 x 和 y 的中点 $\frac{x+y}{2}$ 也属于 C. 下面的定理在泛函分析中起着基本的作用. [285]

定理 II.2.9. — 设 E 为希尔伯特空间, $C\neq\varnothing$ 是 E 的一个闭凸集.

(i) 对任意的 $x\in E$, 存在唯一的 $p_C(x)\in C$ (称为 x 在 C 上的投射) 使得 $d(x,p_C(x))\leqslant d(x,y)$, 其中 $y\in C$ 是任意的元.

(ii) $p_C(x)$ 是 $y\in C$ 中唯一的那种点, 它使得对任意的 $z\in C$ 夹角 $(x-y,z-y)$ 为钝角 (即 $\mathrm{Re}(\langle x-y,z-y\rangle)\leqslant 0$).

(iii) 映射 $x\mapsto p_C(x)$ 满足 1-利普希茨条件.

证明 以 $d(x,C)$ 代表 $d(x,y)$, $y\in C$ 的下确界. 如果 y_1,y_2 是达到此下界的两个点, 让 $z=\frac{y_1+y_2}{2}$, 则 $z\in C$, 从而由中位数恒等式给出

$$\|y_1-y_2\|^2=2\|y_1-x\|^2+2\|y_2-x\|^2-4\|z-x\|^2=4(d(x,C)^2-d(x,z)^2)\leqslant 0.$$

因此有 $y_1=y_2$, 得到了该投射的唯一性.

转而证明存在性[14]. 由 $d(x,C)$ 的定义知存在 C 中的序列 $(y_n)_{n\in\mathbf{N}}$ 使得 $d(x,y_n)$ 当 n 趋向 $+\infty$ 时趋向 $d(x,C)$. 以 $z_{n,m}$ 记 y_n 和 y_m 的中点, 那么, 中位数恒等式给出了

$$\begin{aligned}\|y_n-y_{n+p}\|^2&=2\|y_n-x\|^2+2\|y_{n+p}-x\|^2-4\|z_{n,n+p}-x\|^2\\&\leqslant 2(\|y_n-x\|^2+\|y_{n+p}-x\|^2-2d(x,C)^2).\end{aligned}$$

[13] 注意, 在 $L^2(\mathbf{R}/\mathbf{Z})$ 中的收敛性 (按平方的平均收敛) 并不意味着在任意点都收敛; 事实上, 完全可以事先安排该级数在任一点发散, 除非我们有意使其收敛.

[14] 在有限维情形, 由紧性的一点论证便能得到证明 (习题).

由假设条件知, 不等式右端当 n 趋向 $+\infty$ 而 $p \in \mathbf{N}$ 时趋向 0. 于是 $(y_n)_{n\in\mathbf{N}}$ 是一个柯西序列, 而由于假定了 C 是完备空间中的闭集, 故它收敛于属于 C 的一个元 $p_C(x)$. 由范数的连续性知 $d(x, p_C(x)) = \lim_{n\to+\infty} d(x, y_n) = d(x, C)$. (i) 得证.

设 $z \in C$. 如果 $0 < t < 1$, 则点 $y_t + (1-t)p_C(x) + tz$ 属于 C, 从而

$$\|p_C(x)-x\|^2 \leqslant \|y_t-x\|^2 = \|p_C(x)-x\|^2+t^2\|z-p_C(x)\|^2+2t\mathrm{Re}\langle p_C(x)-x, z-p_C(x)\rangle.$$

令 t 趋向 0, 从而得到不等式 $\mathrm{Re}\langle x-p_C(x), z-p_C(x)\rangle \leqslant 0$. 反之, 如果 $\mathrm{Re}\langle x-y, z-y\rangle \leqslant 0$, 则

$$\|z-x\|^2 = \|y-x\|^2 + \|z-y\|^2 - 2\mathrm{Re}\langle x-y, z-y\rangle \geqslant \|y-x\|^2,$$

这证明了, 如果对任意的 $z \in C$ 有 $\mathrm{Re}\langle x-y, z-y\rangle \leqslant 0$, 则 y 满足定义 $p_C(x)$ 的那些性质. 由此得到 (ii).

最后, 如果 $x, y \in E$, 则由

$$\mathrm{Re}\langle x-p_C(x), p_C(y)-p_C(x)\rangle \leqslant 0,\ \mathrm{Re}\langle y-p_C(x), p_C(x)-p_C(y)\rangle \leqslant 0.$$

取和, 于是得到不等式

$$\mathrm{Re}\langle x-y, p_C(y)-p_C(x)\rangle \geqslant \mathrm{Re}\langle p_C(y)-p_C(x), p_C(y)-p_C(x)\rangle = \|p_C(y)-p_C(x)\|^2.$$

[286] 应用柯西 – 施瓦茨不等式便得到了 (iii) 的证明, 因为按照它有

$$\mathrm{Re}\langle x-y, p_C(y)-p_C(x)\rangle \leqslant |\langle x-y, p_C(y)-p_C(x)\rangle| \leqslant \|x-y\|\cdot\|p_C(y)-p_C(x)\|.$$

□

3. 希尔伯特空间的对偶

在这一小节里, E 代表希尔伯特空间. 如果 $x \in E$, 以 Λ_x 记由 $\Lambda_x(y) = \langle x, y\rangle$ 定义的线性形式.

引理 II.2.10. — 如果 $x \in E$, 则线性形式 Λ_x 连续且 $\|\Lambda_x\| = \|x\|$.

证明　柯西–施瓦茨不等式变为 $|\Lambda_x| \leqslant \|x\|\cdot\|y\|$, 这给出了 Λ_x 的连续性和不等式 $\|\Lambda_x\| \leqslant \|x\|$. 而由 $|\Lambda_x(x)| = \|x\|\cdot\|x\|$ 得到 $\|\Lambda_x\| \geqslant \|x\|$. □

命题 II.2.11. — 设 E 是一个可分的希尔伯特空间.

(i) 如果 A 是 E 的一个子集, 则 A 的正交集 $A^\perp$ (即对于任意的 $a \in A$ 有 $\langle x, a\rangle = 0$ 的 $x \in E$ 的集合) 是 E 的一个闭子向量空间.

(ii) 如果 F 是 E 的一个闭子向量空间, 且 $x \in E$, 则 $x - p_F(x) \in F^\perp$, 并且有[15] $E = F \oplus F^\perp$ 和 $(F^\perp)^\perp = F$.

证明 (i) 由 $\langle x, a\rangle = 0$ 当且仅当 $\Lambda_a(x) = 0$, 又因为 Λ_a 连续, 它的核 H_a 是 E 的一个超平面, 但 $A^\perp = \cap_{a\in A} H_a$, 这证明了 (i).

(ii) 由定义有 $x - p_F(x) \in F^\perp$. 现在, 如果 $x \in F \cap F^\perp$, 则 $\langle x, x\rangle = 0$, 因此 $x = 0$; 由此得到 $F \cap F^\perp = \{0\}$. 另外, $x = (x - p_F(x)) + p_F(x)$, 其中 $x - p_F(x) \in F^\perp$ 而 $p_F(x) \in F$. 由此推出 $E = F + F^\perp$, 从而 $E = F \oplus F^\perp$. 最后, 到闭凸集投射的唯一性表明 $p_{F^\perp}(x) = x - p_F(x)$, 因而 $x = p_F(x) + p_{F^\perp}(x)$. 由于我们还有 $x = p_{F^\perp}(x) + p_{(F^\perp)^\perp}(x)$, 由此得到 $p_{(F^\perp)^\perp}(x) = p_F(x)$, $x \in E$ 任意, 最终有 $(F^\perp)^\perp = F$. □

定理 II.2.12. — (里斯 (Riesz) 定理) 如果 E 是一个可分的希尔伯特空间, 则将 $x \in E$ 对应到线性形式 Λ_x 的映射是从 E 到它的对偶 E^* 的一个等距映射, 这里的 Λ_x 的定义为 $\Lambda_x(y) = \langle x, y\rangle$. 换句话说,

(i) 如果 $x \in E$, 则线性形式 Λ_x 连续且 $\|\Lambda_x\| = \|x\|$. [287]

(ii) 如果 $\Lambda : E \to \mathbf{K}$ 是一个连续的线性形式, 则存在 (唯一的) $x \in E$ 使得 $\Lambda(y) = \langle x, y\rangle$ 对所有的 $y \in E$ 成立.

证明 (i) 已经证明过了 (这是引理 II.2.10 的内容). 先转向 (ii) 的证明[16].

第一个证明. 假定 Λ 非零, 否则只需取 $x = 0$. 设 H 为 Λ 的核, 这是 E 的一个超平面, 由于 Λ 连续, 故它为闭的. 令 $h \in H^\perp$ 非零. 因为 $H \cap H^\perp = \{0\}$, 且 H 是 Λ 的核, 故有 $\Lambda(h) \neq 0$. 设 $y \in E$, 而 $z = y - \frac{\Lambda(y)}{\Lambda(h)}h$. 我们有 $\Lambda(z) = 0$, 即 $z \in H$, 这表明 $\langle h, z\rangle = 0$, 且对所有的 $y \in E$ 有 $\langle h, y\rangle = \frac{\|h\|^2}{\Lambda(h)}\Lambda(y)$. 换而言之, 如果令 $x = \frac{\overline{\Lambda}(h)}{\|h\|^2}h$, 对于任意的 $y \in E$ 我们有 $\Lambda(y) = \Lambda_x(y)$. 得到结论.

第二个证明. 因为假设了 E 是可分的, 所以它与 ℓ^2 等距同构, 故可假定 $E = \ell^2$. 以 e_n, $n \in \mathbf{N}$ 代表 ℓ^2 的标准的希尔伯特基 (即 e_n 是那样的序列, 它除了第 n 项等于 1 外其余全为 0) 并且令 $a_n = \Lambda(e_n)$. 以 $\pi_n : \ell^2 \to \ell^2$ 为映射 $(y_i)_{i\in\mathbf{N}} \mapsto (z_i)_{i\in\mathbf{N}}$, 其中当 $i \leqslant n$ 时 $z_i = y_i$, 而当 $i > n$ 时 $z_i = 0$. 于是 π_n 是线性的, 且因为 $\|\pi_n(y)\|_2 \leqslant \|y\|_2$,

---

[15] 由此定理知, 一个希尔伯特空间的每个闭子空间都有一个闭的补空间. 反之, J. Lindenstrauss 和 L. Tzafriri (1971) 证明了一个具有此性质的巴拿赫空间同构于 ℓ^2.

关于可分巴拿赫空间分类的一个未解决的问题是, 是否 ℓ^2 是唯一的使得它的等距群 (即对任意的 z 满足 $\|u(z)\| = \|z\|$ 的线性双射) 可迁地作用于单位球面 (即对任意的具范数 1 的 x, y, 有一个等距映射 u 使得 $u(x) = y$) 上的这种空间. 在有限维情形, 类似的断言为真: E 的等距映射群 G 是紧的, 因为它在 $\mathrm{GL}(E)$ 中为闭和有界, 因此具有一个哈尔测度, 这便用取平均的方法, 像在定理 I.2.6 中那样构造出一个 G 不变的标量积; 可迁性的假定表明单位球是在此标量积下的球的相似形.

[16] 这是此定理的非平凡部分, 它有泛函分析中一些最精彩的推论. 我们可由它不费力地得到一堆存在性定理.

它也连续, 同时对于所有的 $y \in \ell^2$ 有 $\pi_n(y) \to y$. 设 $\Lambda_n = \Lambda \circ \pi_n$. 进而有

$$\Lambda_n(y) = \Lambda(\sum_{i \leqslant n} y_i e_i) = \sum_{i \leqslant n} a_i y_i = \langle x^{(n)}, y \rangle,$$

其中 $x^{(n)} \in \ell^2$ 的定义为: 当 $i \leqslant n$ 时 $x_i^{(n)} = \overline{a_i}$; 而当 $i > n$ 时 $x_i^{(n)} = 0$. 由 (i) 得到 $\|\Lambda_n\| = \|x^{(n)}\|_2$. 另外, 如果 $y \in \ell^2$, 则因为 $\pi_n(y) \to y$ 及 Λ 连续, 故 $\Lambda_n(y) \to \Lambda(y)$. 从巴拿赫 – 施泰豪斯定理得知 $\|\Lambda_n\|$ 有界因而 $\|x^{(n)}\|_2$ 被函数控制. 这表明 $x = (\overline{a_n})_{n \in \mathbf{N}} \in \ell^2$. 又, $y \mapsto \Lambda'(y) = \Lambda(y) - \langle x, y \rangle$ 是 ℓ^2 上的一个连续线性形式, 它在所有 n 的 e_n 上为 0, 从而因为 e_n 生成了 ℓ^2 的一个稠子空间, 得到它恒等于 0. 证完. □

II.3. 习题

1. 巴拿赫空间

习题 II.3.1. — 设 f 连续且是周期为 1 的周期函数, 而 α 为无理数. 证明

$$\lim_{N \to +\infty} \frac{1}{N} \sum_{n=1}^{N} f(n\alpha) = \int_0^1 f(t)dt.$$

(由一个三角多项式开始.)

习题 II.3.2. — a) 在 $\mathscr{C}_c(\mathbf{R})$ 上的线性形式 $f \mapsto \int_{-\infty}^{+\infty} f(t)dt = I(f)$ 是否可以扩张为 $L^2(\mathbf{R})$ 上的线性形式?

[288] b) 设 e_n 是在 $[0, n]$ 上取值 $\frac{1}{n}$ 而在其余处取值 0 的函数. 证明, $e_n \in L^2(\mathbf{R})$, 且序列 $(e_n)_{n \in \mathbf{N}}$ 在 $L^2(\mathbf{R})$ 中趋向 0. 由此推出, 子空间 $\{f \in \mathscr{C}_c(\mathbf{R}) : I(f) = 0\}$ 在 $L^2(\mathbf{R})$ 中稠密.

c) a) 与 b) 之间有何关系?

习题 II.3.3. — 设 $a = (a_n)_{n \in \mathbf{N}} \in \ell^\infty$ 是一个复数的有界序列.

(i) 证明, 如果 $x = (x_n)_{n \in \mathbf{N}} \in \ell^2$, 则 $(a_n x^n)_{n \in \mathbf{N}} \in \ell^2$, 并且如此定义的线性映射 $f : \ell^2 \to \ell^2$ 连续.

(ii) 证明, 如果 f 为满的, 则存在 $C > 0$ 使得对于所有 $n \in \mathbf{N}$ 有 $|a_n| \geqslant C$ (可以从证明 f 是单的开始).

习题 II.3.4. — (i) 证明, 如果 $a = (a_n)_{n \in \mathbf{N}} \in \ell^\infty$, 而 $b = (b_n)_{n \in \mathbf{N}} \in \ell^1$, 则级数 $\sum_{n \in \mathbf{N}} a_n b_n$ 收敛. 以 $\Lambda_a(b)$ 代表这个级数的和.

(ii) 证明如此定义的映射 $\Lambda_a : \ell^1 \to \mathbf{C}$ 属于 $(\ell^1)^*$, 并且 $\|\Lambda_a\| = \|a\|_\infty$.

(iii) 证明 $a \mapsto \Lambda_a$ 是从 ℓ^∞ 到 $(\ell^1)^*$ 上的一个等距映射. (可从定理 II.2.12 的第二个证明受到启发.)

习题 II.3.5. — 证明一个具有可数个生成元族的巴拿赫空间是有限维的. (如果 $(e_n)_{n\in\mathbf{N}}$ 是这样的族, 则可以考虑由 $i\leqslant n$ 的 e_i 生成的子空间 F_n.)

习题 II.3.6. — 设 I 是 $\mathbf{R}$ 的一个区间, 而 $(f_n)_{n\in\mathbf{N}}$ 是一个 I 上的连续函数的序列, 它单收敛于函数 f. 如果 $j\in\mathbf{N}$, 并设

$$F_{n,j}=\cap_{p\geqslant n}\{x\in I,|f_{n+p}(x)-f_n(x)|\leqslant 2^{-j}\}.$$

(i) 证明 $F_{n,j}$ 为闭集且 $\cup_{n\in\mathbf{N}}F_{n,j}=I$.

(ii) 设 $U_{n,j}$ 是 $F_{n,j}$ 的内核, 而 $U_j=\cup_{n\in\mathbf{N}}U_{n,j}$. 证明 U_j 在 I 中稠密.

(iii) 证明, 如果 $x\in U_j$, 则存在包含 x 的开集 V_x 使得 $|f(x)-f(y)|\leqslant 2^{2-j}$, $y\in V_x$. 由此推出 f 至少在 I 的一个点连续.

2. 希尔伯特空间

习题 II.3.7. — 对于 $f\in L^2([-1,1])$ 的 $\int_{-1}^1 xf(x)dx$ 在条件 $\int_{-1}^1 f(x)dx=1$ 和 $\int_{-1}^1 f(x)^2dx=1$ 下的极大值是什么?

习题 II.3.8. — 设 $(a_n)_{n\in\mathbf{N}}$ 是一个复数的序列, 且满足对于任意的 $(b_n)_{n\in\mathbf{N}}\in\ell^2$ 级数 $\sum_{n=0}^{+\infty}a_nb_n$ 收敛. 证明 $\sum_{n=0}^{+\infty}|a_n|^2<+\infty$. (可考虑线性形式的序列 $\Lambda_k:\ell^2\to\mathbf{C},k\in\mathbf{N}$ 任意, 其定义为 $\Lambda_k((b_n)_{n\in\mathbf{N}})=\sum_{n=0}^k a_nb_n$. 我们可以考虑通项为 $b_n=\frac{\bar{a}_n}{\sum_{i=0}^n|a_i|^2}$ 的级数.)

习题 II.3.9. — 设 E 是一个无限维的希尔伯特空间.

(i) 利用一个无聚点的序列证明 E 的单位球不是紧的.

(ii) 构造 E 的闭子集 F 使得 0 不在 F 的投射上 (就是说, 使得在 F 中不存在具有极小范数的元).

习题 II.3.10. — 设 $(E,\|\ \|)$ 为希尔伯特空间.

(i) 设 a,x,y 是 E 中满足

$$\|x-a\|,\|y-a\|\leqslant r_2 \quad \text{和} \quad \|\frac{x+y}{2}-a\|\geqslant r_1$$

的点. 证明 $\|x-y\|\leqslant 4(r_2^2-r_1^2)$.

(ii) 设 $(C_n)_{n\in\mathbf{N}}$ 是一个非空的闭凸集的序列. 验证 $C=\cap_{n=0}^{+\infty}C_n$ 是一个闭凸集. [289] 证明, C 非空当且仅当 $\sup_{n\in\mathbf{N}}d(0,C_n)<+\infty$. 特别地, 可证明在此条件下, 当 $x\in E$ 时, $P_{C_n}(x)$ 趋向 $P_C(x)$.

(iii) 设 $\varphi:E\to\mathbf{R}$ 是一个凸函数 (即, 对于任意的 $t\in[0,1]$ 和 $x,y\in E$, 有 $\varphi(tx+(1-t)y)\leqslant t\varphi(x)+(1-t)\varphi(y)$ 成立) 使得 $\lim_{\|x\|\to\infty}\varphi(x)=+\infty$. 证明, φ 在 E 上有下界并达到极小.

习题 II.3.11. — 设 E 为希尔伯特空间, 而 $(e_n)_{n\in\mathbf{N}}$ 是一个法正交族, 设 $(a_n)_{n\in\mathbf{N}}$ 为一个正的实数序列. 证明 $C = B(0,1) \cap \{\sum_{n=0}^{+\infty} x_n e_n, x_n \in [-a_n, a_n]\}$ 是一个紧集当且仅当 $\sum_{n=0}^{+\infty} a_n^2 < +\infty$.

习题 II.3.12. — (勒让德多项式) 以 P_n 记多项式 $\frac{d^n}{dx^n}(1-x^2)^n$. 证明这些 P_n 构成 $L^2([-1,1])$ 中的一个正交族, 而 $P_n/\|P_n\|_2$ 构成 $L^2([-1,1])$ 的一个希尔伯特基.

习题 II.3.13. — 设 E 为希尔伯特空间, 而 $A: E \to E$ 为对所有 $x, y \in E$ 满足 $\langle Ax, y\rangle = \langle x, Ay\rangle$ 的线性映射, 证明 A 连续. (利用习题 II.1.27 的结果.)

习题 II.3.14. — 设 $L^2([0,1])$ 为 $\mathscr{C}([0,1])$ 在标量积 $\langle f, g\rangle = \int_0^1 \overline{f(t)} g(t) dt$ 的完备化.

(i) 设 $X_1, \ldots, X_n$ 为变量. 证明矩阵 $(\frac{1}{X_i+X_j})_{1\leqslant i,j\leqslant n}$ 的行列式是

$$\Delta_n(X_1, \ldots, X_n) = \frac{\prod_{i<j}(X_i - X_j)^2}{\prod_{i,j}(X_i + X_j)}.$$

(ii) 设 $1 \leqslant a_1 < a_2 < \cdots$ 是一个严格递增的整数序列, 如果 $n \in \mathbf{N}$, 以 $\mathrm{Vect}(x^{a_1}, \ldots, x^{a_n})$ 记 $\mathscr{C}([0,1])$ 中由这些 $x^{a_i}, 1 \leqslant i \leqslant n$ 生成的子空间. 证明, 如果 $k \in \mathbf{N}$, 则

$$d(x^k, \mathrm{Vect}(x^{a_1}, \ldots, x^{a_n}))^2 = \frac{\Delta_{n+1}(k+\frac{1}{2}, a_1+\frac{1}{2}, \ldots, a_n+\frac{1}{2})}{\Delta_n(a_1+\frac{1}{2}, \ldots, a_n+\frac{1}{2})}.$$

(iii) 证明 $\mathrm{Vect}(x^{a_i}, i \in \mathbf{N})$ 在 $L^2([0,1])$ 中稠密当且仅当 $\sum_{n=1}^{+\infty} \frac{1}{a_i} = +\infty$.

习题 II.3.15. — (i) 设 $\mathscr{C}_c([1,+\infty[)$ 为 $\phi: [1,+\infty[\to \mathbf{C}$ 的具紧支集的连续函数的空间. 证明 $(f,g) \mapsto \langle f, g\rangle = \int_1^{+\infty} \overline{f(t)} g(t) \frac{dt}{t^2}$ 是 $\mathscr{C}_c([1,+\infty[)$ 上的一个标量积, 而且在此标量积下 $\mathscr{C}_c([1,+\infty[)$ 不是完备的.

(ii) 以 E 记 $\mathscr{C}_c([1,+\infty[)$ 在此标量积下的完备化. 如果 n 为 $\geqslant 2$ 的一个整数, 令 $\phi_n: [1,+\infty[\to \mathbf{C}$ 为函数 $\phi_n(t) = [\frac{t}{n}] - \frac{[t]}{n}$. 证明 $\phi_n \in E$.

(iii) 证明由这些 ϕ_n, $n \geqslant 2$ 在 E 中生成的子空间的闭包包含了 $[1,+\infty[$ 上的常值函数的空间. (提示: 参看习题 VII.5.2.)

3. 傅里叶级数

习题 II.3.16. — 设 f 是一个周期 1 的周期函数使得当 $x \in]-\frac{1}{2}, \frac{1}{2}]$ 时 $f(x) = x$. 计算 f 的傅里叶系数; 并由此得到 $\sum_{n=1}^{+\infty} \frac{1}{n^2}$ 的值.

设 $f \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$, 且当 $N \in \mathbf{N}$ 时令 $\Lambda_N(f) = \sum_{k=-N}^{N} c_k(f)$. 更一般地, 当 $x \in \mathbf{R}/\mathbf{Z}$ 时令 $\Lambda_{N,x}(f) = \sum_{k=-N}^{N} c_k(f) e^{2i\pi kx}$. 我们的目的是研究 f 的傅里叶级数的对称部分和 $\Lambda_{N,x}(f)$ 趋向 $f(x)$ 的收敛性.

作为初始的问题, 我们要证明 Λ_N 是 $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ 上的一个连续的线性形式, 并建立公式 $\Lambda_N(f) = \int_0^1 S_N(t) f(t) dt$, 其中 $S_N(t) = \frac{\sin(2N+1)\pi t}{\sin \pi t}$.

习题 II.3.17. — (i) 证明 $\|\Lambda_N\| = \|S_N\|_1$. [290]

(ii) 证明 $\|\Lambda_N\|$ 趋向 $+\infty$; 由此推出 $\{f \in \mathscr{C}(\mathbf{R}/Z), \sup_{N\in\mathbf{N}} |\Lambda_N(f)| = +\infty\}$ 是一个稠密于 $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ 的 G_δ 集.

(iii) 证明, 如果 $r \in \mathbf{Q}$, 则满足 $\sup_{N\in\mathbf{N}} |\Lambda_{N,r}(f)| = +\infty$ 的 $f \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$ 的集合是 $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ 中的一个稠的 G_δ 集. 由此推出存在 $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ 中一个稠的 G_δ 集 X 使得对于任意的 $f \in X$ 和 $r \in \mathbf{Q}$ 有 $\sup_{N\in\mathbf{N}} |\Lambda_{N,r}(f)| = +\infty$.

(iv) 证明, 如果 $f \in X$, $M \in \mathbf{N}$, 则使得 $\sup_{N\in\mathbf{N}} |\Lambda_{N,x}(f)| > M$ 的 $x \in \mathbf{R}/\mathbf{Z}$ 的集合是一个包含 $\mathbf{Q}/\mathbf{Z}$ 的开集. 由此推出, 如果 $f \in X$, 则存在一个稠密于 $\mathbf{R}/\mathbf{Z}$ 的 G_δ 集 Y_f 使得 $\sup_{N\in\mathbf{N}} |\Lambda_{N,x}(f)| = +\infty$, 其中任意 $x \in Y_f$[17].

习题 II.3.18. — 设 $L^1(\mathbf{R}/\mathbf{Z})$ 是 $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ 在范数 $\|f\|_1 = \int_0^1 |f(t)|dt$ 下的完备化.

(i) 证明, 如果 $k \in \mathbf{Z}$, 则 $f \mapsto c_k(f)$ 可连续地延拓到 $L^1(\mathbf{R}/\mathbf{Z})$.

(ii) 证明, 如果 $f \in L^1(\mathbf{R}/\mathbf{Z})$, 则当 $|k| \to +\infty$ 时 $c_k(f) \to 0$.

(iii) 假设 f 对于某个 $\alpha > 0$ 存在 $C > 0$ 使得对于任意的 $x, y \in [0,1]$ 有 $|f(x) - f(y)| \leqslant C|x-y|^\alpha$ (也称为指数 α 的赫尔德不等式). 证明, 如果 $x \in \mathbf{R}$, 则通项为 $\sum_{k=-N}^{N} c_k(f)e^{2i\pi kx}$ 的序列趋向 $f(x)$.

II.4. p-adic 巴拿赫空间

1. 定义和例题

一个 p-adic 巴拿赫空间是在 $\mathbf{Q}_p$ 上的一个巴拿赫空间[18], 但因为 $\mathbf{Q}_p$ 上的范数是超度量的, 自然也要赋予这个空间这种范数, 这让我们有以下的定义.

定义 II.4.1. — 一个 p-adic 巴拿赫空间是一个 $\mathbf{Q}_p$-向量空间 E, 其上有一个超度量 $\|\ \|$ (即 $\|x+y\| \leqslant \sup(\|x\|, \|y\|)$ 和 $\|\lambda x\| = |\lambda|_p \|x\|$, 其中 $\lambda \in \mathbf{Q}_p$, $x, y \in E$), 并在此范数下完备.

注记 II.4.2. — (i) 如果 E 是一个 p-adic 巴拿赫空间, 范数的超度量性使得单位球 $E^0 = \{x \in E, \|x\| \leqslant 1\}$ 是 E 的一个加法子群, 并在乘以 $\mathbf{Z}_p$ 中的元下稳定 (即它是 $\mathbf{Q}_p$ 向量空间 E 的一个 $\mathbf{Z}_p$-模).

(ii) 范数的超度量性和空间的完备性使得一个级数 $\sum_{i\in I} x_i$ 在 E 中收敛当且仅 [291]

---

[17] 换句话说, 存在 $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ 的一个稠的不可数子集使得, 如果 $f \in X$, 则 f 的傅里叶级数在 $\mathbf{R}/\mathbf{Z}$ 的一个稠的不可数子集的每点发散. 尽管这个结果并不令人鼓舞, 但 Carlson (2006 年的阿贝尔奖得主) 还是在 1965 年证明了, 如果 $f \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$ (甚至 $f \in L^2(\mathbf{R}/Z)$), 则对几乎所有的 x (在下面一章的意义下) 有 $\Lambda_{N,x}(f) \to f(x)$. 另一方面, 科尔莫戈罗夫 (1926) 证明了存在 $L^1(\mathbf{R}/\mathbf{Z})$ 中的元的傅里叶变换在每点都发散.

[18] 同样地我们可以考虑在 $\mathbf{R}$ 和 $\mathbf{C}$ 上的巴拿赫空间, 可以将 $\mathbf{Q}_p$ 换做任何一个对于 p-adic 范数的完备域, 如像 $\mathbf{Q}_p$ 的有限扩域或是 $\mathbf{C}_p$.

当在无限远 $x_i \to 0$[19].

定义 II.4.3. (假设条件) — 称 E 满足假设条件 (N) 是说, 对于任意的 $x \in E$, 存在 $\lambda \in \mathbf{Q}_p$ 使得 $\|x\| = |\lambda|_p$

引理 II.4.4. — 如果 $(E, \|\ \|)$ 是一个 p-adic 巴拿赫空间, 则可以找到 E 上的一个范数 $\|\ \|_1$ 等价于 $\|\ \|$, 并满足假设条件 (N).

证明　如果 $x \in E$, 令 $v_p(x)$ 为满足 $\|x\| = p^{-v_p(x)}$ 的 $\mathbf{R} \cup \{+\infty\}$ 中的一个元, 再令 $\|x\|_1 = p^{-[v_p(x)]}$, 其中当 $v \in \mathbf{R}$ 时, $[v]$ 代表 v 的整数部分. 于是 $\|\ \|_1$ 是 E 上的一个超度量, 并进一步成立 $\frac{1}{p}\|x\|_1 \leqslant \|x\| \leqslant \|x\|_1$. □

例题 II.4.5. — (i) 设 I 是一个集合, 令 $\ell^\infty(I)$ 是 $\mathbf{Q}_p$ 中的有界序列 $(a_i)_{i\in I}$ 的集合. 赋予 $\ell^\infty(I)$ 一个范数 $\|\ \|_\infty$ 为 $\|(a_i)_{i\in I}\|_\infty = \sup_{i\in I} |a_i|_p$, 使它成了一个 p-adic 巴拿赫空间.

(ii) 设 $\ell_0^\infty(I)$ 为 $\ell^\infty(I)$ 的一个子空间, 它由其中的在无限远趋向 0 的 $(a_i)_{i\in L}$ 构成. 它作为一个 p-adic 巴拿赫空间的闭子空间是一个 p-adic 巴拿赫空间. 它也是只具有有限个非零项的序列的集合在 $\ell^\infty(I)$ 中的闭包.

(iii) 如果 X 是一个紧的拓扑空间, $\mathscr{C}(X)$ 代表从 X 到 $\mathbf{Q}_p$ 的连续映射的集合, 并赋予它范数 $\|\ \|_\infty : \|\phi\|_\infty = \sup_{x\in X} |\phi(x)|_p$, 于是它是一个 p-adic 巴拿赫空间.

(iv) 在附录 D 中可以找到更多的有趣例子.

2. 法正交基

p-adic 巴拿赫空间的理论比起这个空间的阿基米德同调而言还远不是那么丰富; 它与希尔伯特空间的理论尤其相近. 特别地, 下面的概念可替代希尔伯特空间中的希尔伯特基的概念.

定义 II.4.6. — 设 E 是一个 p-adic 巴拿赫空间. 称一个有界族 $(e_i)_{i\in I}$ 是 E 的一个法正交基是说 $(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i e_i$ 是从 $\ell_0^\infty(I)$ 到 E 上的一个等距映射. 称它是一个巴拿赫基是说这个映射是一个 p-adic 巴拿赫空间之间的一个同构 (一个法正交基因而是一个巴拿赫基).

换句话说, 一个族 $(e_i)_{i\in I}$ 是 E 的一个法正交基当且仅当

(i) E 的每个元都可以以唯一的方式写成一个收敛级数 $x = \sum_{i\in I} a_i e_i$ 的形式, 这里的 a_i 是 $\mathbf{Q}_p$ 的元, 并在无限远趋向 0.

(ii) $\|x\| = \sup_{i\in I} |a_i|$.

它是一个巴拿赫基表明它有界并满足条件 (i), 根据开映像定理这表明有以下性

[19] 一个族 $(x_i)_{i\in I}$ 在无限远趋向 0 是说, 对所有的 $\varepsilon > 0$ 有 $\{i, \|x_i\| \geqslant \varepsilon\}$ 为有限集 (应该说成是 "按照有限子集的补集的滤形趋向 0", 但这有点笨拙 ……).

质: [292]

(ii') 存在常数 $C \geqslant 1$ 使得有

$$C^{-1} \sup_{i \in I} |a_i| \leqslant \|x\| \leqslant C \sup_{i \in I} |a_i|.$$

例题 II.4.7. — (i) 如果 $i \in I$, 令 $e_i = (e_{i,j})_{j \in I}$, 其中 $e_{ii} = 1$ 而当 $j \neq i$ 时 $e_{i,j} = 0$. 由定义, 所有 $e_i, i \in I$ 构成 $\ell_0^\infty(I)$ 的一个法正交基.

(ii) 对于 $n \in \mathbf{N}$ 的 $\binom{x}{n}$ 构成了 $\mathscr{C}(\mathbf{Z}_p)$ 的法正交基: 这是马勒定理的简单翻译 (定理 20.4 和注记 20.5).

命题 II.4.8. — (i) 所有的 p-adic 巴拿赫空间都具有巴拿赫基.

(ii) 一个 p-adic 巴拿赫空间具有法正交基当且仅当它满足假设条件 (N). 另外在此假设条件下. $(e_i)_{i \in I}$ 是 E 的法正交基当且仅当 $(\bar{e}_i)_{i \in I}$ 是 $\mathbf{F}_p$-向量空间 $\overline{E} = E^0/pE^0$ 的一个代数基, 其中 $E^0 = \{x \in E, \|x\| \leqslant 1\}$ 是 E 的单位球.

证明 引理 II.4.4 表明 (i) 是 (ii) 的推论. 因而可设 E 满足假设条件 (N), 在此条件下证明 $(e_i)_{i \in I}$ 是 E 的一族法正交基当且仅当 $(\bar{e}_i)_{i \in I}$ 是在 $\mathbf{F}_p$-向量空间 $\overline{E}$ 上的一族代数基.

设 $(e_i)_{i \in I}$ 是 E^0 的一族元使得 $(\bar{e}_i)_{i \in I}$ 是 $\mathbf{F}_p$-向量空间 $\overline{E}$ 的基. 令 $S = \{0, 1, \ldots, p-1\}$ 以及 $s : \mathbf{F}_p \to S$ 为 $\bmod p$ 约化的逆. 如果 $x \in E^0$, 则可将其 $\bmod p$ 的像 $\bar{x}$ 写为有限和 $\sum_{i \in I} a_i \bar{e}_i$, 其中 a_i 为 $\mathbf{F}_p$ 中几乎处处为零的元. 令 $s(x) = \sum_{i \in I} s(a_i) e_i$. 那么由构造有 $x - s(x) \in pE^0$.

如果 $x \in E^0$, 我们归纳地定义一个 E^0 的序列 $(x_n)_{n \in \mathbf{N}}$ 为: $x_0 = x$, $x_{n+1} = \frac{1}{p}(x_n - s(x_n))$. 于是对于任意的 $k \in \mathbf{N}$ 有 $x = \sum_{n=0}^{k} p^n s(x_n) + p^{k+1} x_{k+1}$, 从而 $x = \sum_{n \in \mathbf{N}} p^n s(x_n)$. 另外, $s(x_n) = \sum_{i \in I} s_{n,i} e_i$, 其中这些 $s_{n,i}$ 是 S 中几乎处处为零的元, 这表明, 如果令 $a_i = \sum_{n=0}^{+\infty} p^n s_{n,i}$, 则 a_i 的序列在无限远趋向 0 (如果对于 $n \leqslant k-1$ 有 $s_{n,i} = 0$, 则 $|a_i|_p \leqslant p^{-k}$ 对几乎所有 i 成立). 因此有 $x = \sum_{i \in I} a_i e_i$, 这证明了映射 $(a_i)_{i \in I} \mapsto \sum_{i \in I} a_i e_i$ 是从 ℓ_0^∞ 到 E 的一个满映射. 如果 $\boldsymbol{a} = (a_i)_{i \in I} \in \ell_0^\infty(I)$ 满足 $\|\boldsymbol{a}\|_\infty = 1$, 则存在 $i \in I$ 使得 $a_i \notin p\mathbf{Z}_p$, 而因为这些 $\bar{e}_i$, $i \in I$ 构成 $\overline{E}$ 的基, 故 $\sum_{i \in I} a_i e_i \neq 0 \mod p$. 这表明 $1 \geqslant \|\sum_{i \in I} a_i e_i\| > p^{-1}$, 并且因为已经假设了条件 (N), 故由此得到 $\|\sum_{i \in I} a_i e_i\| = 1$, 从而映射 $(a_i)_{i \in I} \mapsto \sum_{i \in I} a_i e_i$ 是从 $\ell_0^\infty(I)$ 到 E 上的一个等距映射. 这证明了, 如果 $\bar{e}_i$, $i \in I$ 是 $\overline{E}$ 的一组基, 则这些 e_i, $i \in I$ 便是 E 的一个法正交基.

现假设这些 e_i, $i \in I$ 是 E 的一个法正交基. 如果 $x \in \overline{E}$, 则可选取 $\tilde{x} \in E^0$ 使其 $\bmod p$ 的像为 x. 由于 $\|\tilde{x}\| \leqslant 1$, 故 $\tilde{x}$ 可以以唯一的方式写为形式 $\tilde{x} = \sum_{i \in I} a_i e_i$, $a_i \in \mathbf{Z}_p$, 其中 $\mathbf{Z}_p$ 在无限远趋向 0. 因此得到 a_i 的 $\bmod p$ 约化 $\bar{a}_i$ 除了有限个 i 外全为 0 (我们有 $\bar{a}_i \neq 0$ 当且仅当 $|a_i|_p = 1$), 以及 $x = \sum_{i \in I} \bar{a}_i \bar{e}_i$ 是一个 $\bar{e}_i$ 的线性组合; 这些 $\bar{e}_i$ 因此构成了 $\overline{E}$ 的一个生成元族. 最后, 如果在 $\overline{E}$ 中 $\sum_{i \in I} a_i \bar{e}_I = 0$, 且如果 $\tilde{a}_i \in \mathbf{Z}_p$ 的 $\bmod p$ 像为 a_i, 则 $x = \sum_{i \in I} \tilde{a}_i e_i \in pE^0$, 从而 $\|x\| < 1$. 由于 $\|x\| = \sup_{i \in I} |\tilde{a}_i|_p$, [293]

这表明 $|\tilde{a}_i|_p < 1$, 故 $a_i = 0$, $i \in I$. 于是得到 $\bar{e}_i$ 是一个无关族, 从而是 $\overline{E}$ 的基.

证完. □

3. p-adic 巴拿赫空间的对偶

如果 E 是一个 p-adic 巴拿赫空间, 以 E^* 代表它的对偶 (即 E 到 $\mathbf{Q}_p$ 的连续线性形式). 像通常那样, 一个线性形式 $\Lambda : E \to \mathbf{Q}_p$ 连续当且仅当存在 $C > 0$ 使得 $|\Lambda(x)|_p \leqslant C\|x\|$, $x \in E$, 并定义 Λ 的范数 $\|\Lambda\|$ 为满足上面不等式的 C 的下确界; 它是 Λ 的算子范数, 同时也有 $\|\Lambda\| = \sup_{x \in E-\{0\}} \|x\|^{-1}|\Lambda(x)|_p$. 这赋予 E^* 一个超度量范数 (超度量性是 $|\ \|_p$ 的超度量性的推论), 并从定理 II.1.28 得到, E^* 在此范数下是完备的; 因此它是一个 p-adic 巴拿赫空间.

命题 II.4.9. — 设 I 是一个集合.

(i) 如果 $\boldsymbol{b} = (b_i)_{i \in I} \in \ell^\infty(I)$, 且 $\boldsymbol{a} = (a_i)_{i \in I} \in \ell_0^\infty(I)$, 则级数 $\sum_{i \in I} a_i b_i$ 在 $\mathbf{Q}_p$ 中收敛.

(ii) 如果 $\Lambda_{\boldsymbol{b}}(\boldsymbol{a})$ 代表级数 $\sum_{i \in I} a_i b_i$ 的和, 则映射 $\boldsymbol{b} \mapsto \Lambda_{\boldsymbol{b}}$ 是从 $\ell^\infty(I)$ 到 $\ell_0^\infty(I)$ 的对偶上的等距映射.

证明 (i) 此级数的收敛性来自 $a_i b_i$ 在无限远趋向 0: 因为 a_i 在无限远趋向 0 而 b_i 有界.

(ii) 直接可得 $\Lambda_{\boldsymbol{b}}$ 的线性性和等式 $\|\Lambda_{\boldsymbol{a}}\| = \|\boldsymbol{b}\|_\infty$. 因此证明了映射 $\boldsymbol{b} \mapsto \Lambda_{\boldsymbol{b}}$ 的满性: 设 $\Lambda \in \ell_0^\infty(I)^*$. 由于 Λ 连续, 如果令 $b_i = \Lambda(\delta_i)$, 则有 $|b_i|_p \leqslant \|\Lambda\|$, 这证明 $\boldsymbol{b} = (b_i)_{i \in I} \in \ell^\infty(I)$. 然而由此得到 $\Lambda - \Lambda_{\boldsymbol{b}}$ 在 ℓ_0^∞ 的由 δ_i 生成的子空间上取零, 又因为它在 $\ell_0^\infty(I)$ 中稠密, 而 $\Lambda - \Lambda_{\boldsymbol{b}}$ 连续, 故 $\Lambda = \Lambda_{\boldsymbol{b}}$. 证完. □

III. 积分

III.1. 勒贝格积分

勒贝格积分 (1902—1904) 是黎曼积分[1] 的一个具有极端可塑性的推广 (更可以说成是一个完备). 可积函数的空间变成了完备的[2], 这大大地简化了积分的存在或收敛问题. 由于勒贝格控制收敛定理 (定理 III.1.32), 给出了使积分和极限交换的非常强有力的工具. 黎曼积分所有的经典的断言 (依赖一个参数的积分的连续性和可微性, 富比尼定理) 均可推广到此而且其证明常常得到简化. 然而对那些已经证明存在的积分, 要明晰地计算出来却常常是困难的.

1. 砌块与阶梯函数

设 $\mathbf{Z}[\frac{1}{2}]$ 是二进位数 (即分母为 2 的幂次的有理数) 的环. $\mathbf{R}^m$ 中的一个*砌块*是 $\mathbf{R}^m$ 的一个形如[3] $\prod_{j=1}^m [r_j, s_j[$ 的子集, 其中对于 $1 \leqslant j \leqslant m$, 有 $r_j < s_j$ 为二进位数. 一个*铺砌*是有限个砌块的并. 一个 (2^{-r} 大小的) *初等砌块*是一个形如 $D_{r,\boldsymbol{k}}$ 的集合, 其中 $r \in \mathbf{N}$, $\boldsymbol{k} = (k_1, \ldots, k_m) \in \mathbf{Z}^m$, 而 $D_{r,\boldsymbol{k}} = \prod_{j=1}^m [\frac{k_j}{2^r}, \frac{k_j+1}{2^r}[$.

引理 III.1.1. — (i) *如果 D_1 和 D_2 为初等砌块 (不必具同样大小), 则或者 D_1 和 D_2 不交或者一个包含在另一个之中*[4].

(ii) *如果 $\boldsymbol{k} \in \mathbf{Z}^m$, 则 $D_{r,\boldsymbol{k}}$ 是 $D_{r+1,2\boldsymbol{k}+\boldsymbol{a}}$, $\boldsymbol{a} \in \{0,1\}^m$ 的不交并.*

---

[1] 黎曼积分是在 1854 年出现的; 它推广了柯西积分, 后者对于 (一致) 连续函数有定义 (1823 年在巴黎综合理工大学的课程上给出), 参看小词典的习题 16.5.

[2] 甚至, 如果必要可诉诸选择公理, 让所有不太粗糙的函数 (譬如在一个有界集上有界) 是可积的 (参看脚注 14).

[3] 请读者就 $m = 1$ 或 $m = 2$ 的情形作图; 这可使得后面的断言变得完全清晰起来.

[4] 换而言之, 初等砌块就像是水银珠.

(iii) 每个砌块是有限个同样大小的初等砌块的不交并.

[296] 证明 留作习题. □

我们定义一个初等砌块 $D_{r,\boldsymbol{k}}$ 的测度 $\lambda(D_{r,\boldsymbol{k}})$ 为 $\lambda(D_{r,\boldsymbol{k}}) = 2^{-mr}$. 如果 D 是一个任意的铺砌, 并设其为对 $i \in I$ 有限集的 $D_{r,\boldsymbol{k}_i}$ 的不交并, 则定义 $\lambda(D) = \sum_{i\in I}\lambda(D_{r,\boldsymbol{k}_i})$. 应用上面的引理的 (ii), 可证明这个定义不依赖所选的覆盖 D 的初等砌块的大小.

如果 $r \in \mathbf{N}$ 且 $\boldsymbol{k} \in \mathbf{Z}^m$, 以 $e_{r,\boldsymbol{k}}$ 表示 $D_{r,\boldsymbol{k}}$ 的特征函数. 如果 $r \in \mathbf{N}$, 我们以 $\mathrm{Esc}_r(\mathbf{R}^m)$ 记 $e_{r,\boldsymbol{k}}$, $\boldsymbol{k} \in \mathbf{Z}^m$ 的线性组合形成的向量空间, 它是 $\mathbf{R}^m$ 上的阶梯函数的集合, 这些函数在大小为 2^{-r} 的初等砌块上为常值. 对于 $\boldsymbol{k} \in \mathbf{Z}^m$ 的这些 $e_{r,\boldsymbol{k}}$ 是线性无关的 (如果 $x \in \mathbf{R}^m$, 则恰好存在一个 $\boldsymbol{k} \in \mathbf{Z}^m$ 使得 $e_{r,\boldsymbol{k}}(x) \neq 0$), 它们形成了 $\mathrm{Esc}_r(\mathbf{R}^m)$ 的一组基.

由于 $e_{r,\boldsymbol{k}} = \sum_{\boldsymbol{a}\in\{0,1\}^m} e_{r+1,2\boldsymbol{k}+\boldsymbol{a}}$, 我们有 $\mathrm{Esc}_r(\mathbf{R}^m) \subset \mathrm{Esc}_{r+1}(\mathbf{R}^m)$, 其中 $r \in \mathbf{N}$. 这些 $\mathrm{Esc}_r(\mathbf{R}^m)$ 对于 $r \in \mathbf{N}$ 的并 $\mathrm{Esc}(\mathbf{R}^m)$ 因此是一个向量空间; 称其为 $\mathbf{R}^m$ 上的阶梯函数的向量空间. (注意, 线性组合是一个有限和, 故一个阶梯函数是具紧支集的[5].)

如果 $X \subset \mathbf{R}^m$, 以 $\mathrm{Esc}(X)$ 记 X 上的阶梯函数; 可以将它看作是 $\mathbf{R}^m$ 上的阶梯函数但它在 X 外取零值. 更一般地, 如果 $X \subset \mathbf{R}^m$, 而 $U \subset \mathbf{C}$, 以 $\mathrm{Esc}(X, U)$ 记 X 上的取值在 $U \subset \mathbf{C}$ 的阶梯函数的集合. 因此, $\mathrm{Esc}(X) = \mathrm{Esc}(X, \mathbf{C})$.

如果 $\phi \in \mathrm{Esc}(\mathbf{R}^m)$, 则存在 $r \in \mathbf{N}$ 使得可以将 ϕ 写成 $\phi = \sum_{i\in I}\alpha_i e_{r,\boldsymbol{k}_i}$. 那么我们定义它的积分 $\int\phi$ 为 $\int\phi = \sum_{i\in I}\alpha_i\lambda(D_{r,\boldsymbol{k}_i}) = 2^{-rm}\sum_{i\in I}\alpha_i$. 利用公式 $e_{r,\boldsymbol{k}} = \sum_{\boldsymbol{a}\in\{0,1\}^m} e_{r+1,2\boldsymbol{k}+\boldsymbol{a}}$, 可证明此定义不依赖 r 的选取, 从而如此便定义了 $\mathrm{Esc}(\mathbf{R}^m)$ 上的一个线性形式. 根据上下文, ϕ 的积分可随便地记为以下的任意一种:

$$\int\phi = \int_{\mathbf{R}^m}\phi = \int_{\mathbf{R}^m}\phi d\lambda \int_{\mathbf{R}^m}\phi(x)dx = \int_{\mathbf{R}^m}\phi(x)dx_1\cdots dx_m.$$

注记 III.1.2. — 如果 $\phi \in \mathscr{C}_c(\mathbf{R}^m)$ 是具紧支集的连续函数, 并且如果以 ϕ_r 记对任意的 $\boldsymbol{k} \in \mathbf{Z}^m$ 的阶梯函数 $\sum_{\boldsymbol{k}\in\mathbf{Z}^m}\phi(\frac{\boldsymbol{k}}{2^r})e_{r,\boldsymbol{k}}$, 它在初等砌块 $\prod_{j=1}^m[\frac{k_j}{2^r}, \frac{k_j+1}{2^r}[$ 取值 $\phi(\frac{k_1}{2^r}, \ldots, \frac{k_m}{2^r})$, 因此在范数 $\|\ \|_\infty$ 下 $\phi_r \to \phi$(一致地[6]). 它让我们证明了序列 $(\int\phi_r)_{r\in\mathbf{N}}$ 收敛, 故可定义黎曼积分 $\int\phi$ 为这个序列的极限. 勒贝格积分将以同样的方式定义, 但放弃了[7]一致收敛的条件, 代之以条件: 几乎处处单收敛.

[297] 2. 零测度集

定义一个集合 A 的外测度 $\lambda^+(A)$ 为对于满足 $A \subset \cup_{n\in\mathbf{N}}D_n$ 的 $\sum_{n\in\mathbf{N}}\lambda(D_n)$ 的下确界, 其中 $(D_n)_{n\in\mathbf{N}}$ 是遍历 $\mathbf{R}^m$ 中砌块的序列. 分解这些砌块 D_n 为大小随 n 增

[5] ϕ 的支集是那些 x 使得 $\phi(x) \neq 0$ 的集合的闭包; 由定义, 这是个闭集.

[6] 这是在一个紧集上的连续函数为一致连续的推论.

[7] 由于一致收敛性表明了几乎处处单收敛 (见后面的定义), 那么具有紧支集的连续函数的黎曼积分和勒贝格积分重合, 因而勒贝格积分是黎曼积分的推广.

大而递降的初等砌块, 并消去那些包含在某个 D_i, $i \leqslant n-1$ 中的 D_n 的初等砌块, 则化成了这些 D_n 是互不相交的初等砌块的情形 [8].

命题 III.1.3. — (i) 如果 $B \subset A$, 则 $\lambda^+(B) \leqslant \lambda^+(A)$.

(ii) 如果 $A_n \subset \mathbf{R}^m$, $n \in \mathbf{N}$, 则 $\lambda^+(\cup_{n\in\mathbf{N}} A_n) \leqslant \sum_{n\in\mathbf{N}} \lambda^+(A_n)$.

证明 (i) 显然. (ii) 当 $\sum_{n\in\mathbf{N}} \lambda^+(A_n) = +\infty$ 时也是显然的. 在相反的情形下, 设 $A = \cup_{n\in\mathbf{N}} A_n$, 而 $\varepsilon > 0$. 对于每个 $n \in \mathbf{N}$, 可以找到 $\mathbf{R}^m$ 中的铺砌的一个序列 $(D_{n,k})_{k\in\mathbf{N}}$ 使得 $A_n \subset \cup_{k\in\mathbf{N}} D_{n,k}$, 以及 $\sum_{k\in\mathbf{N}} \lambda(D_{n,k}) \leqslant \lambda^+(A_n) + 2^{-1-n}\varepsilon$. 然而我们因此有了 $A \subset \cup_{k,n\in\mathbf{N}} D_{n,k}$ 和

$$\sum_{k,n\in\mathbf{N}} \lambda(D_{n,k}) \leqslant \sum_{n\in\mathbf{N}} (\lambda^+(A_n) + 2^{-1-n}\varepsilon) = \varepsilon + \sum_{n\in\mathbf{N}} \lambda^+(A_n)$$

由此得到 $\lambda^+(A) \leqslant \varepsilon + \sum_{n\in\mathbf{N}} \lambda^+(A_n)$, $\varepsilon > 0$ 任意, 这使我们得到了结论. □

我们称 A 是零测度的是说它满足 $\lambda^+(A) = 0$. 回到定义, 我们便看出 A 为零测度当且仅当对于任意的 $\varepsilon > 0$ 存在 $\mathbf{R}^m$ 中一个砌块的序列 $(D_n)_{n\in\mathbf{N}}$ 使得 $A \subset \cup_{n\in\mathbf{N}} D_n$ 且 $\sum_{n\in\mathbf{N}} \lambda(D_n) < \varepsilon$.

命题 III.1.4. — (i) 一个零测度的集合的每个子集仍是零测度的.

(ii) 可数个零测度集的并仍是零测度的.

证明 是命题 III.1.3 的直接推论. □

习题 III.1.5. — 证明如果 A 为 $\mathbf{R}^n$ 中的零测度集, 则 $A \times \mathbf{R}^m$ 是 $\mathbf{R}^{n+m}$ 中的零测度集.

习题 III.1.6. — (i) 证明 $\mathbf{R}^2$ 中的对角线为零测度集.

(ii) 更一般地, 证明连续映射 $f : \mathbf{R} \to \mathbf{R}$ 在 $\mathbf{R}^2$ 中的图为零测度集, 又 $\mathbf{R}^m$ 中的超平面是零测度的.

(iii) $[0, 1]$ 在到 $\mathbf{R}^2$ 的连续映射下的像一定是零测度的吗?

我们说某个性质几乎处处为真, 或者对几乎所有的点 $x \in \mathbf{R}^m$ 为真, 再或者为真 p.p.[42]是指不满足这个性质的点集为零测度的. 例如, 因有理数的集合可数, 故实数几乎处处是无理数. 同样, 几乎所有的复数都是超越数[9]. (称一个复数是代数的是 [298]

[8]这个结果让人不禁想起在计算机上显现图像的方式.

[9]由于这些结果, 一个数如果不是代数的则必是超越的, 但证明一个给定的数是超越的或者即便是无理的, 一般说来, 是非常困难的. 例如, 一直到 1979 年, R.Apéry 才证明了 $\zeta(3)$ 是个无理数, 对于 $\geqslant 5$ 的奇整数 n, 之前我们还不知道如何证明 $\zeta(n)$ 是无理的. 在这个方向上仅有的结果是 T.Rivoal(2000) 的, 他证明了 $\zeta(n)$ 对于无限多个奇整数 n 是无理的, 且至少九个数 $\zeta(5), \ldots, \zeta(21)$ 中有 1 个数是无理的 (之后 W.Zudilin 有所改进: 至少有 4 个数 $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ 是无理的).

[42]在国内一般都用英文中的 "a.e.(almost everywhere)" 来替代法文中的 "p.p.", 这里也如此; 但有时在中文中放在尾部不合习惯, 还不如直接文字表达. 我有时直接用中文 "几乎处处", 有时采用 "a.e.".

说它是一个系数在 $\mathbf{Q}$ 中的首 1 多项式的根. 称一个非代数的复数是超越数.)

注记 III.1.7. — (i) 不要相信 $\mathbf{R}$ 的一个零测度子集必定是可数的. 譬如, 固定一个 $\mathbf{N}$ 到 $\mathbf{Q}$ 的双射 $n \mapsto r_n$, 并令 $U_k = \cup_{n\in\mathbf{N}}]r_n - 2^{-n-k}, r_n + 2^{-n-k}[$, $k \in \mathbf{N}$, 而 $A = \cap_{k\in\mathbf{N}} U_k$. 因为对所有的 k, A 包含在 U_k 中, 且 $\lambda^+(U_k) \leqslant \sum_{n=0}^{+\infty} 2^{1-n-k} = 2^{2-k}$ 可以任意地小, 故 A 为零测度集. 另一方面, 对于每个 k, U_k 是一个稠开集, 那么根据贝尔引理 (参看小词典的 14.2 小节), A 稠密且不可数. 特别地, A 包含除了有理数以外的数, 从其构造上看这并不完全显见.

(ii) 一个零测度集可能有十分令人吃惊的性质. 譬如, A. Besicovitch (1919) 构造了 $\mathbf{R}^m$, $m \geqslant 2$ 中的一些零测度集, 它们包含了在所有方向上的一个长度为 1 的线段[10].

习题 III.1.8. — 证明几乎处处为零的一个连续函数恒等于零.

定理 III.1.9. — (博雷尔–坎泰利 (Borel-Cantelli)) *如果 $(a_n)_{n\in\mathbf{N}}$ 是 $\mathbf{R}_+$ 中的序列使得 $\sum_{n\in\mathbf{N}} a_n < +\infty$, 且如果 $(A_n)_{n\in\mathbf{N}}$ 是 $\mathbf{R}^m$ 中的一个子集的序列, 它对于每个 $n \in \mathbf{N}$ 满足 $\lambda^+(A_n) \leqslant a_n$, 则几乎所有的 $x \in \mathbf{R}^m$ 只属于有限个 A_n.*

证明　需要证明属于无限多个 A_n 的 $x \in \mathbf{R}^m$ 的集合 A 为零测度的. 但 $x \in A$ 当且仅当对所有的 $n \in \mathbf{N}$, 存在 $p \geqslant n$ 使得 $x \in A_p$; 换而言之, 我们有 $A = \cap_{n\in\mathbf{N}}(\cup_{p\geqslant n} A_p)$. 由此推出 $\lambda^+(A) \leqslant \sum_{p\geqslant n} \lambda^+(A_p)$, 其中 $n \in \mathbf{N}$ 任意, 并且由于级数 $\sum_{n\in\mathbf{N}} \lambda^+(A_n)$ 假设为收敛的, 它的余项因而趋向 0. 证完. □

[299] **习题 III.1.10.** — (i) 证明, 如果 $\varepsilon > 0$ 以及 $C > 0$, 则对于几乎所有[11] 的实数 x, 满足 $|x - \frac{p}{q}| \leqslant Cq^{-2-\varepsilon}$ 的整数偶 (p, q) 的集合有限.

(ii) 证明刘维尔数的集合的测度为零, 并且在 $\mathbf{R}$ 中稠密. (一个实数 x 是刘维尔的[12] 是说, 它不是一个有理数, 并且对任何的 $n \in \mathbf{N}$, 存在一堆整数 (p, q), $q \geqslant 2$ 使得

---

[10] 这些集合是分析中令人讨厌的反例的来源 (譬如对于维数 $\geqslant 2$ 的傅里叶级数的收敛性问题). 如果能够证明 (Kakeya 问题) 一个 Besicovitch 集不是太大的话, 这些分析问题便会是相当令人满意的了, 更准确地说, $\mathbf{R}^m$ 中的一个 Besicovitch 集具有闵可夫斯基维数 m: 一个集合的闵可夫斯基维数是指 $\frac{\log N(X,k)}{\log k}$ 当 $k \to +\infty$ 时的极限 (如果存在), 其中 $N(X, k)$ 是完全覆盖 X 的所需要的半径为 $\frac{1}{k}$ 的球的最小个数. 目前所知的最好结果属于 N. Katz 和陶哲轩 (2001): $\mathbf{R}^m$ 中的 Besicovitch 集的闵可夫斯基维数至少是 $(2 - \sqrt{2})(m - 4) + 3$, $m > 4$.

[11] K. Roth (1955) 证明了那个让他获得了菲尔兹奖的结果, 即代数数具有这个性质 (对于有理数或者次数为 2 的代数数这是显然的 (如果 α 是个代数数, α 的次数是满足 $P(\alpha) = 0$ 的非零多项式 $P \in \mathbf{Q}[X]$ 的最小次数), 但一般的情形则需展示出绝活才行). 还不知道 π 是否满足这个性质. 以同样的想法, 如果 x 是一个非有理的实数, 则可取它的连分式展开式 (它是一个由以下算法定义的整数序列 $(a_n)_{n\in\mathbf{N}}$: $x_0 = x, a_n = [x_n], x_{n+1} = \frac{1}{x_n - a_n}$; 由将 x 用 $a_0, \ldots, a_{n-1}$ 和 x_n 写出并再次在表达式中将 x_n 换作 a_n, 这样得到的这些有理数 $\frac{u_n}{v_n}$ 是 x 用有理数的最好近似). 容易证明, 对几乎所有的实数 x, 序列 a_n 不是有界的, 这等价于集合 $\{q|qx - p| : p, q \in \mathbf{Z}, q \geqslant 1\}$ 的下确界为零. 如果 x 是 2 次的代数数, 则级数 a_n 从某一项开始成为周期的, 因而有界. 实际上, 我们相信, 如果 x 是次数 $\geqslant 3$ 的代数数, 则序列 a_n 不是有界的, 但是我们不知道对任何一种情形的证明.

[12] 这些数是刘维尔在 1844 年引进的, 它们被证明为超越的首批的数; e 的超越性是在 1873 年被证明的 (埃尔米特), 而 π 的证明则是在 1882 年 (林德曼 (Lindemann)).

$|x-\frac{p}{q}|\leqslant q^{-n}$.)

3. 可测函数, 可测集合

3.1. 可测函数

称一个函数 $f:\mathbf{R}^m\to\mathbf{C}$ (分别地, $f:\mathbf{R}^m\to\overline{\mathbf{R}}_+$) 为可测的是说, 它是一个阶梯函数序列的几乎处处收敛的极限. 换句话说, f 可测是指存在零测度的集合 $A\subset\mathbf{R}^m$ 以及一个 $\mathrm{Esc}(\mathbf{R}^m)$(分别地, $\mathrm{Esc}(\mathbf{R}^m,\mathbf{R}_+)$) 中的序列 $(f_n)_{n\in\mathbf{N}}$ 使得对所有的 $x\notin A$ 有 $f_n(x)\to f(x)$.

以 $\mathrm{Mes}(\mathbf{R}^m)$ 代表 $\mathbf{R}^m$ 上取值于 $\mathbf{C}$ 中的可测函数的集合. 更一般地, 如果 $D\subset\mathbf{R}^m$, $F\subset\mathbf{C}$ (或 $F\subset\overline{\mathbf{R}}_+$), 我们以 $\mathrm{Mes}(D,F)$ 记 $\mathbf{R}^m$ 上的那些可测函数的集合, 它们在 D 外为 0 而取值在 F 中.

- 常值函数可测 (函数 λ 是 $\lambda\mathbf{1}_{D_N}$ 的极限, 其中 D_N 是砌块 $[-N,N[^m$).
- $\mathrm{Mes}(\mathbf{R}^m)$ 是一个 $\mathbf{C}$-代数 (即对于 $\lambda\in\mathbf{C}$ 以及 f,g 可测, 有 $\lambda f, f+g$ 和 fg 可测). 事实上, 如果 $(f_n)_{n\in\mathbf{N}}$ 和 $(g_n)_{n\in\mathbf{N}}$ 是 $\mathrm{Esc}(\mathbf{R}^m)$ 中的序列, 它们在 A_f 和 A_g 外分别趋向 f 和 g, 其中的 A_f 和 A_g 为零测度集, 于是:

  — 在 A_f 之外 $\lambda f_n\to\lambda f$, 从而 λf 可测.

  — 在 $A_f\cup A_g$ (仍为零测度) 外 $f_n+g_n\to f+g$, 从而 $f+g$ 可测.

  — 在 $A_f\cup A_g$ 外 $f_ng_n\to fg$, 从而 fg 可测.
- 如果 $f,g\in\mathrm{Mes}(\mathbf{R}^m,\overline{\mathbf{R}}_+)$, 则 $\inf(f,g)$ 和 $\sup(f,g)$ 可测. 事实上, 如果 $(f_n)_{n\in\mathbf{N}}$ [300] 和 $(g_n)_{n\in\mathbf{N}}$ 是 $\mathrm{Esc}(\mathbf{R}^m,\overline{\mathbf{R}}_+)$ 中的序列, 且它们分别在零测度集 A_f 和 A_g 之外趋向 f 和 g, 于是在 $A_f\cup A_g$ 之外 $\inf(f_n,g_n)$(分别地, $\sup(f_n,g_n)$) 趋向 $\inf(f,g)$(分别地, $\sup(f,g)$).
- $f:\mathbf{R}^m\to\mathbf{C}$ 可测当且仅当这些函数[13] $\mathrm{Re}^+(f)$, $\mathrm{Re}^+(-f)$, $\mathrm{Re}^+(if)$ 和 $\mathrm{Re}^+(-if)$ 都可测: $f=\mathrm{Re}^+(f)-\mathrm{Re}^+(-f)-i\mathrm{Re}^+(if)+i\mathrm{Re}^+(-if)$, 由此得到了蕴含关系: "$\mathrm{Re}^+(f)$, $\mathrm{Re}^+(-f)$, $\mathrm{Re}^+(if)$ 和 $\mathrm{Re}^+(-if)$ 可测" ⇒"f 可测". 反方向的关系来自: 如果 g 为阶梯函数, 则 $\mathrm{Re}^+(g)$ 也是, 以及 Re^+ 连续.

习题 III.1.11. — (i) 证明, 如果 f 在 $\mathbf{R}^n$ 上可测, 而 g 在 $\mathbf{R}^m$ 上可测, 则 $h(x,y)=f(x)g(y)$ 在 $\mathbf{R}^{n+m}$ 上可测.

(ii) 证明连续函数可测.

命题 III.1.12. — 可测函数的几乎处处收敛的单极限仍然可测.

证明 这个命题并不是像看起来那么显然 (参看习题 II.1.11). 证明将在 §III.4 的 4 小

[13] 如果 $z\in\mathbf{C}$, 我们以 $\mathrm{Re}^+(z)$ 记实数 $\sup(0,\mathrm{Re}(z))$; 因此有

$$z=\mathrm{Re}^+(z)-\mathrm{Re}^+(-z)+i\mathrm{Re}^+(-iz)-i\mathrm{Re}^+(iz).$$

节给出. □

习题 III.1.13. — (i) 证明一个函数可测当且仅当它是一个连续函数的序列的几乎处处收敛的单极限.

(ii) 由此推出连续函数的几乎处处收敛的单极限的几乎处处收敛的单极限是一个连续函数序列的几乎处处收敛的单极限. 请与习题 II.1.11 比较.

3.2. 可测集系

• 称 $\mathbf{R}^m$ 的子集 X 可测是说它的特征函数 $\mathbf{1}_X$ 是一个可测函数[14]. 特别地:

— 一个零测度集可测 (它的特征函数是每项为零的序列的几乎处处收敛的单极限).

— 如果 A 和 B 可测, 则 $A \cap B$ 和 $A \cup B$ 可测 (事实上, 我们有 $\mathbf{1}_{A\cap B} = \inf(\mathbf{1}_A, \mathbf{1}_B)$, $\mathbf{1}_{A\cup B} + \sup(\mathbf{1}_A, \mathbf{1}_B)$).

[301] **习题 III.1.14.** — 证明, 如果 X 在 $\mathbf{R}^n$ 中可测, 而 Y 在 $\mathbf{R}^m$ 中可测, 则 $X \times Y$ 在 $\mathbf{R}^{n+m}$ 中可测.

• 如果 E 是一个集合, E 的一个集系 $\mathscr{A}$ 是 E 的子集的一个非空集合, 其在取补集时稳定 (如果 $A \in \mathscr{A}$, 则 $E - A \in \mathscr{A}$), 并且取可数并时稳定 (如果 I 可数, 且 $(A_i)_{i\in I}$ 为 $\mathscr{A}$ 中的元族, 则 $\cup_{i\in I} A_i \in \mathscr{A}$). 一个集系总包含 E 和 $\emptyset$ (如果 $A \in \mathscr{A}$, 则 $A \cup (E - A) \in \mathscr{A}$), 并且因为 $\cap_{i\in I} A_i$ 是 A_i 的补的并, 它在可数交下也稳定.

• E 上集系的交仍为集系, 从而如果 $\mathscr{B}$ 是 E 的子集的一个集合便可定义由 $\mathscr{B}$ 生成的集系为包含 $\mathscr{B}$ 的所有集系的交.

• 如果 E 是一个拓扑空间 (譬如, $E = \mathbf{R}, \mathbf{R}^m, \overline{\mathbf{R}}_+, \dots$), E 上的博雷尔集系 $\mathscr{B}or$ 是指由所有开集, 或者等价地, 所有的闭集生成的集系. 称博雷尔集系中的一个元为一个博雷尔集; 开集和闭集都是博雷尔集, 但要描述任意一个博雷尔集是非常困难的[15]. 在 $\mathscr{B}or$ 的子集中我们特别提及可数个开集的交的集合 $\mathscr{G}_\delta$ 和可数个闭集的并的集合 $\mathscr{F}_\sigma$.

• $\mathbf{R}^m$ 的博雷尔集系也是由初等砌块生成的集系. 事实上, $\mathbf{R}^m$ 的一个开集是它包含的砌块的并, 并且它们是可数的, 这证明开集是在由初等砌块生成的集系之中, 从而包含了 $\mathscr{B}or$. 反过来, 砌块 $\prod_{i=1}^m [\frac{k_i}{2^r}, \frac{k_i+1}{2^r}[$ 是开集 $\prod_{i=1}^m]-\infty, \frac{k_i+1}{2^r}[$ 和闭集

[14] 巴拿赫和塔斯基 (Tarski)(1924) 构造了 $\mathbf{R}^3$ 中的半径为 1 的一个球的分成有限块的剖分 (5 块足够), 使得如果重新安排这些块 (即以 $\mathbf{R}^3$ 中的等距映射移动这些块), 则得到半径为 1 的两个球 (巴拿赫-塔斯基悖论); 其中这些块不是可测的, 但在这里, 巴拿赫和塔斯基用了选择公理.

另一方面, R. Solovay (1966) 证明了, 如果禁用不可数的选择公理, 但保留可数的选择公理, 则能够假定所有的集合都是可测的而不会在数学上添加矛盾. 由此结果得到的训诫是, 实践上, 在分析中所遇到的所有函数从而所有集合都是可测的, 而且不用浪费时间去求证它们是可测的; 但在概率论中则有所不同, 那里同一个事件根据条件可以是可测的也可以是不可测的.

[15] 无论以什么方式, 一个显式的描述对应用而言是完全无用的: 我们证明对任意一个博雷尔集具某个性质在于验证它当取补时为真, 取可数并时为真, 以及对于开集为真即可 (或者对生成 $\mathscr{B}or$ 的 $\mathscr{B}or$ 的任何一个元族验证).

$\prod_{i=1}^{m}[\frac{k_i}{2^r},+\infty[$ 的交, 因此是 $\mathscr{B}or$ 中的元; 于是得到 $\mathscr{B}or$ 包含了所有的初等砌块从而包含了它所生成的集系.

习题 III.1.15. — 设 $(f_n)_{n\in\mathbf{N}}$ 是从 $\mathbf{R}^m$ 到 $\mathbf{C}$ 的连续函数的序列.

(i) 证明 $\{x\in\mathbf{R}^m, f_n(x)\to 0\}$ 是一个博雷尔集.

(ii) 证明 $\{x\in\mathbf{R}^m, f_n(x)\text{有极限}\}$ 是一个博雷尔集 (考虑柯西判别准则).

我们称 A 和 B 只差一个零测度集是说 $\mathbf{1}_A=\mathbf{1}_B$ 几乎处处成立, 这等价于说 $A-(A\cap B)$ 和 $B-(A\cap B)$ 都是零测度集.

定理 III.1.16. — *(i) 可测集构成 $\mathbf{R}^m$ 上的一个集系.*

(ii) 可测集的集系是由博雷尔集和零测度集生成的集系[16]. 更准确地说, 以下的条件等价:

- *X 可测,*
- *存在 $G\in\mathscr{G}_\delta$ 使得 X 和 G 只相差一个零测度集,*
- *存在 $F\in\mathscr{F}_\sigma$ 使得 X 和 F 只相差一个零测度集.*

证明　如果 X 可测, 因为它的补的特征函数为 $1-\mathbf{1}_X$ 是可测函数的线性组合, 从而其补集可测. 如果这些 $(X_i)_{i\in\mathbf{N}}$ 可测, 则它们并的特征函数是函数 $\sup_{i\leqslant n}\mathbf{1}_{X_i}$ 的单极限, 因此, 作为可测函数的单极限仍然是可测的.

由此证明了 (i). 为了证明 (ii), 我们首先注意, 一个博雷尔集是可测的: 因为一 [302] 个初等砌块是可测的而由初等砌块生成的集系就是由博雷尔集生成的集系. 由于一个零测度集也是可测的, 故可测集的集系包含了由博雷尔集和零测度集生成的集系. 要证明反向的包含关系只要证明一个可测集具有一个定理中所描述的其中一个就可以了. 如果 $(f_k)_{k\in\mathbf{N}}$ 是一个在零测度集 A 之外单收敛于 $\mathbf{1}_X$ 的阶梯函数序列, 那么当 X_k 是那些满足 $|f_k(x)-1|\leqslant\frac{1}{2}$ 的 $x\in\mathbf{R}^m$ 的砌块时, 则在 A 外仍有 $\mathbf{1}_{X_k}\to\mathbf{1}_X$. 令 U_k 为 X_k 的内核. 由于 X_k-U_k 包含在初等砌块的面的并集中, 从而是一个零测度集, 故存在一个零测度集 A' 使得在 A' 之外有 $\mathbf{1}_{U_k}\to\mathbf{1}_X$. 于是得到 $\mathbf{1}_X(x)=\limsup\mathbf{1}_{U_k}(x)$, $x\notin A'$, 从而 X 与 $G=\cap_{n\in\mathbf{N}}\cup_{k\geqslant n}U_k$ 相差一个零测度集, 并且因为 $\cup_{k\geqslant n}U_k$ 为开集, 故 $G\in\mathscr{G}_\delta$, 这给出了所要的第一个描述. 第二个只需取补集便可. 证完. □

3.3. 可测函数和可测集

根据脚注 14, 所有正常的函数和集合都是可测的 (对不正常的集合可参看习题 III.1.27), 但如果不愿意使用这个元定理来检验一个函数的可测性, 那么下面的结果则提供了一个方便的判别法.

命题 III.1.17. — *如果 $f:\mathbf{R}^m\to\overline{\mathbf{R}}_+$, 则下面的条件等价:*

[16] 用基数论证法可以证明存在可测的但不是博雷尔集的集合: 博雷尔集的集合的基数与 $\mathbf{R}$ 相同, 而可测集的集合却包含了康托尔集的子集的集合, 它的基数严格地更大.

- f 可测,
- 对于 $\overline{\mathbf{R}}_+$ 的所有的博雷尔集 X, $f^{-1}(X)$ 可测,
- 对于所有的 $a \in \mathbf{R}_+$, $f^{-1}([0,a[)$ 可测,
- 对于所有的 $a \in \mathbf{R}_+$, $f^{-1}([0,a])$ 可测.

证明 后面的 3 个 • 的等价性来自 $\mathbf{R}_+$ 的博雷尔集系是由这些 $[0,a[$ 或这些 $[0,a]$, $a \in \mathbf{R}_+$ 生成的这个事实. 所以只要证明第一个 • 和第三个 • 等价即可. 如果 $f^{-1}([0,a[)$ 对所有的 $a \in \mathbf{R}_+$ 可测, 则 $X_{n,k} = f^{-1}([\frac{k}{2^n}, \frac{k+1}{2^n}[) = f^{-1}([0, \frac{k+1}{2^n}[) - f^{-1}([0, \frac{k}{2^n}[)$ 也可测, 其中 $n, k \in \mathbf{N}$. 于是作为可测函数 (即级数) 的单极限的 $f_n = \sum_{k\in\mathbf{N}} \frac{k}{2^n}\mathbf{1}_{X_{n,k}}$ 是可测的, 又因为 f_n 单趋向 f, 故 f 可测.

反过来, 设 f 可测, 并设 $(f_k)_{k\in\mathbf{N}}$ 是 $\mathrm{Esc}(\mathbf{R}^m, \mathbf{R}_+)$ 中在零测度集 B 之外趋向 f 的一个序列. 如果 $b \in \mathbf{R}_+$, 令 $D_{b,k} = f_k([0,b[)$, 而 $X_b = f^{-1}([0,b[)$, $X_b^+ = f^{-1}([0,b])$. 于是 $D_{n,k}$ 是个砌块, 从而 $Y_b = \cap_{n\in\mathbf{N}} \cup_{k\geqslant n} D_{n,k}$ 可测. 另外, 如果 $x \in X_b - B$, 则 $f(x) < b$, 从而对于充分大的 k 有 $f_k(x) < b$, 因此 $X_b - B \subset Y_b$. 同样地, 如果 $x \in Y_b - B$, 当 k 趋向无穷时 $f_k(x) < b$ 则 $f(x) \leqslant b$; 换而言之, $Y_b - B \subset X_b^+$. 由于 B 为零测度的, 于是得知存在一个可测的 Y_b', 它仅与 Y_b 差一个零测度集, 使得 $X_b \subset Y_b' \subset X_b^+$. 如果 a_n 是一个以 a 为极限的递增序列, 则有 $X_a = \cup_{n\in\mathbf{N}} Y'_{a_n}$, 这证明了作为可测集的可数并的 X_a 是可测的. 证完. □

4. 勒贝格积分的定义

一旦定义了一个可测函数, 问题便是如何度量它. 勒贝格积分 (和勒贝格测度) 为 [303] 许多问题提供了一个自然度量. 我们选取的表述纯粹是公理化的[17]; 它不是那种在预备班的课程上采用的涉及实数时的观点 (在那里 $\mathbf{R}$ 表示了一个全序域, 其中所有的非空子集都具有上确界, 在 $\mathbf{R}$ 的这个表述中具有上确界这个性质所起的作用在这里由单调收敛性取代).

4.1. 正函数的积分

定理 III.1.18. — 存在一个从 $\mathrm{Mes}(\mathbf{R}^m, \overline{R}_+)$ 到 $\overline{\mathbf{R}}_+$ 的映射 $f \to \int f$, 它满足如下的性质 (i)—(v).

(i) 如果 f 为阶梯函数, 则 $\int f$ 是前面已定义过的那个量.

(ii)(线性性) $\int(af+bg) = a\int f + b\int g$, 其中 $a, b \in \mathbf{R}_+$, $f, g \in \mathrm{Mes}(\mathbf{R}^m, \overline{\mathbf{R}}_+)$.

(iii) $\int f = 0$ 当且仅当 $f = 0$ a.e.

(iv) 如果 $f \leqslant g$ a.e., 则 $\int f \leqslant \int g$.

(v) (单调收敛定理) 如果 (f_n) 是一个 $\mathrm{Mes}(\mathbf{R}^m, \overline{\mathbf{R}}_+)$ 中元的递增序列, 则

[17] 它的优点是可略去一些十分细微的点块而不会降低应用这个理论的便利. 然而为了减少一些精力充沛的数学家对于使用了一个没有看到 (或者忘掉) 证明的结果的念头而感到有点不舒服的感觉, 我们在 §III.4 中构造了满足这个公理的积分.

$\lim_{n\to+\infty}\int f_n(x)=\int\lim_{n\to+\infty}f_n$.

注记 III.1.19. — (i) 积分的线性性 (性质 (ii)) 和单调收敛定理 (性质 (v)) 是基本性质.

(ii) 性质 (iv) 可由 (ii) 和 (iii) 导出: 事实上, 我们有 $\int g+\int -\inf(0,g-f)=\int f+\int\sup(g-f,0)$, 其中的所有函数均为正的, 于是按假设条件, 有 $-\inf(0,g-f)=0$ a.e.

(iii) 性质 (i) 规范了定义在 $\mathbf{R}^m$ 上的一个特别的测度, 即勒贝格测度. 如我们将看到的 (定理 III.3.8), 这个性质表明了勒贝格测度在平移下的不变性. 反过来, 如果 $f\mapsto\int f$ 为线性的和平移下不变的 (这意味对所有的 $f\in\mathrm{Mes}(\mathbf{R}^m,\overline{\mathbf{R}_+})$ 和 $a\in\mathbf{R}^m$, 有 $\int T_a(f)=\int f$, 其中 $(T_a(f))(t)=f(t+a)$), 并且如果 $\int e_{0,\mathbf{0}}=1$, 则根据平移下的不变性, $\int e_{r,\boldsymbol{k}}$ 不依赖 $\boldsymbol{k}$, 那么由规范化 $\int e_{0,\mathbf{0}}=1$ 知其取值 2^{-rm}(用对 r 的归纳由此得到 $\int e_{r,\boldsymbol{k}}$ 对于 $\boldsymbol{k}$ 的无关性和公式 $e_{r,\boldsymbol{k}}=\sum_{\boldsymbol{a}\in\{0,1\}}^m e_{r+1,\boldsymbol{k}+\boldsymbol{a}}$); 线性性因此蕴含了 $\int f$ 满足性质 (i). 换而言之, 我们可以将性质 (i) 换为平移不变性和规范性 $\int e_{0,\mathbf{0}}=1$[18].

4.2. 集合的勒贝格测度 [304]

如果 $X\subset\mathbf{R}^m$ 可测, 它的勒贝格测度定义为 $\lambda(X)=\int\mathbf{1}_X\in\overline{\mathbf{R}}_+$. 下面的结果证明勒贝格测度对可数个元是可加的, 从而定义了具有一个可测集集系的 $\mathbf{R}^m$ 上的一个测度[19].

命题 III.1.20. — 如果 $(X_i)_{i\in I}$, I 为可数集, 是 $\mathbf{R}^m$ 中的一些不交的可测子集, 则

$$\lambda(\cup_{i\in I}X_i)=\sum_{i\in I}\lambda(X_i).$$

证明 X_i 为两两不交的假设可化为 $\mathbf{1}_{\cup_{i\in I}X_i}=\sum_{i\in I}\mathbf{1}_{X_i}$, 那么如有必要可将 I 中的元排序, 从而应用单调收敛定理 (在 I 为无限时) 到部分和 $\sum_{i\leqslant n}\mathbf{1}_{X_i}$ 即可. □

命题 III.1.21. — 设 $f\in\mathrm{Mes}(\mathbf{R}^m,\overline{\mathbf{R}}_+)$.

(i) $\int f=0$ 当且仅当 $\lambda(\{t,f(t)\neq 0\})=0$.

(ii) 如果 $\int f<+\infty$, 则 $\lambda(\{t,f(t)=+\infty\})=0$.

证明 如果 $A=\{t,f(t)\neq 0\}$. 则对所有的 $N\in\mathbf{N}$, $\inf(f,N)\leqslant N\mathbf{1}_A$ 从而 $\int\inf(f,N)\leqslant N\lambda(A)$. 由于 $\inf(f,N)$ 递增地趋向 f, 故由单调收敛定理可以证明当 $\lambda(A)=0$ 时 $\int f=0$. 反过来, 如果 $\int f=0$, 则对所有的 N 有 $\int Nf=N\int f=0$. 由于 Nf 递增地趋向 $+\infty\mathbf{1}_A$, 那么单调收敛定理表明 $+\infty\lambda(A)=0$, 故 $\lambda(A)=0$. (i) 得证.

---

(18) 这个方法可以推广到所有的局部紧群上, 包括 $\mathbf{R}^m$, 有限群, 紧群, $\mathbf{Z}$, 加法群 $\mathbf{Q}_p$, 乘法群 $\mathbf{R}^*$, $\mathbf{C}^*$ 或者 $\mathbf{Q}_p^*$, 或更一般地, 当 $d\geqslant 1$ 时的群 $\mathbf{GL}_d(\mathbf{R}),\mathbf{GL}_d(\mathbf{C}),\mathbf{GL}_d(\mathbf{Q}_p)$ 和它们的闭子群 ……. 一个这样的群在差一个 $\geqslant 0$ 的乘法常因子下, 具有唯一的右 (分别地, 左) 不变测度, 这表明 $\int T_a^d(f)=\int f$ (分别地, $\int T_a^g(f)=\int f$, 其中 $(T_a^d(f))(x)=f(xa^{-1})$, $(T_a^g(f))(x)=f(ax)$; 这个测度是右 (分别地, 左) 哈尔测度.

(19) 在具有一个集系 $\mathscr{A}$ 的 E 上, 一个集合的测度 μ 是一个函数 $\mu:\mathscr{A}\to\overline{\mathbf{R}}_+$, 它满足 $\mu(\emptyset)=0$, 以及对于 $\mathscr{A}$ 中的元的两两不交的可数族 $(X_i)_{i\in I}$ 有 $\mu(\cup_{i\in I}X_i)=\sum_{i\in I}\mu(X_i)$.

要证明 (ii) 只要注意到, 如果 $A=\{t,f(t)=+\infty\}$, 对于任意的 $M\in\mathbf{R}_+$ 我们有 $f\geqslant M\mathbf{1}_A$, 则所有任意的 $M\in\mathbf{R}_+$ 我们有 $M\lambda(A)\leqslant\int f$. □

推论 III.1.22. — X 为零测度当且仅当 $\lambda(X)=0$.

证明 设 $X\subset\mathbf{R}^m$, 于是

$$X \text{ 为零测度集} \Leftrightarrow \mathbf{1}_X=0\ a.e. \Leftrightarrow \int \mathbf{1}_X=0 \Leftrightarrow \lambda(X)=0.$$

第一个等价关系是定义, 第二个来自定理 III.1.18 的 (iii), 而最后一个则由命题 III. 1.21 的 (i) 得到. □

推论 III.1.22 是在 §III.4 的 2 小节中将证明的下面结果的特殊情形.

定理 III.1.23. — 如果 X 可测, 则 $\lambda(X)=\lambda^+(X)$.

习题 III.1.24. — 设 $X_n\subset\mathbf{R}^m$ 对于 $n\in\mathbf{N}$ 可测, 且 $B=\cup_{n\in\mathbf{N}}X_n$ 和 $C=\cap_{n\in\mathbf{N}}X_n$.

(i) 证明如果序列 X_n 递增, 则 $\lambda(B)=\lim_{n\to+\infty}\lambda(X_n)$.

(ii) 证明如果序列 X_n 递减, 且 $\lambda(X_0)<+\infty$, 则 $\lambda(C)=\lim_{n\to+\infty}\lambda(X_n)$. 这个结果在没有条件 $\lambda(X_0)<+\infty$ 下成立吗?

[305] **习题 III.1.25.** — 设 $X\subset\mathbf{R}^m$ 是一个具有有限测度的可测集. 证明对于任意的 $\alpha\in[0,1]$, 存在可测集 $B\subset X$ 使得 $\lambda(B)=\alpha\lambda(X)$.(可以考虑 $f(t)=\lambda(X\cap[-t,t]^m)$.)

习题 III.1.26. — (i) 回到定义, 证明 $\lambda^+([0,1])=1$(测度论的基本定理: $\lambda^+([0,1])\neq 0$ 并非是明显的 ……).

(ii) $\mathbf{R}^m$ 的一个铺块是一个形如 $\prod_{j=1}^m I_j$ 的集合, 其中 I_j 是任意形状的区间 (每个端点或开或闭). 证明如果 $P=\prod_{j=1}^m I_j$ 是一个铺块, 则它的外测度由 $\lambda^+(P)=\prod_{j=1}^m\lambda(I_j)$ 给出, 其中 $\lambda(I_j)$ 是区间 I_j 的长 (即, 如果 $a\leqslant b$ 为两个实数, 则 $\lambda(]a,b[)=\lambda([a,b[)=\lambda(]a,b])=\lambda([a,b])=b-a$).

习题 III.1.27. — 证明如果 $S\subset[0,1]$ 是 $\mathbf{R}/\mathbf{Q}$ 的一个代表系 (即 $\mathbf{R}$ 中的所有元可以以唯一的方式写为形式 $s+q$, 其中 $s\in S$ 而 $q\in Q$), 于是 S 不可测. 与脚注 14 比较.

4.3. 可和函数的积分

将任意一个函数分解为它的正负实部和正负虚部, 让我们可以定义一个取值于 $\mathbf{C}$ 的任意函数的积分, 但是由于 $+\infty-(+\infty)$ 没有意义, 我们必须限制所考虑的函数的集合.

定义 III.1.28. — (勒贝格积分)

(i) 如果 $\int|f|<+\infty$, 则称 $f\in\mathrm{Mes}(\mathbf{R}^m)$ 可和. 以 $\mathscr{L}^1(\mathbf{R}^m)\subset\mathrm{Mes}(\mathbf{R}^m)$ 为可和函数的集合.

(ii) 如果 $f\in\mathscr{L}^1(\mathbf{R}^m)$, 于是由于有控制函数 $|f|$, 故 $\mathrm{Re}^+(f),\mathrm{Re}^+(-f),\mathrm{Re}^+(if)$

和 $\mathrm{Re}^+(-if)$ 均可和. 令

$$\int f = \int \mathrm{Re}^+(f) - \int \mathrm{Re}^+(-f) + i\int \mathrm{Re}^+(-if) - i\int \mathrm{Re}^+(if).$$

注记 III.1.29. — (i) 积分 $f \mapsto \int f$ 是 $\mathbf{C}$-线性的: 形式地由定理 III.1.18 得到. (对于 $\lambda \in \mathbf{R}$ 或者 $\lambda = i$, 可直接得到 $\int \lambda f = \lambda \int f$; 因而唯一的问题是证明 $\int f + g = \int f + \int g$; 按照分解为正负虚实部, 问题化为证明当 f, g 为正时的 $\int f - g = \int f - \int g$. 令 $A = \{x, f(x) \geqslant g(x)\}$, $B = \{x, f(x) < g(x)\}$. 于是按定义, $\int f - g = \int (f - g)\mathbf{1}_A - \int (g-f)\mathbf{1}_B$. 由于 $(f-g)\mathbf{1}_A + g\mathbf{1}_A = f\mathbf{1}_A$, 故有 $\int (f-g)\mathbf{1}_A + \int g\mathbf{1}_A = \int f\mathbf{1}_A$, 因此 $\int (f-g)\mathbf{1}_A = \int f\mathbf{1}_A - \int g\mathbf{1}_A$. 同样地, $\int (g-f)\mathbf{1}_B = \int g\mathbf{1}_B - \int f\mathbf{1}_B$, 因此 $\int (f-g)\mathbf{1}_A - \int (g-f)\mathbf{1}_B = \int f\mathbf{1}_A - \int g\mathbf{1}_A + \int f\mathbf{1}_B - \int g\mathbf{1}_B = \int f - \int g$: 因为 $f = f\mathbf{1}_A + f\mathbf{1}_B$, $g = g\mathbf{1}_A + g\mathbf{1}_B$.)

(ii) 如果 f 可和, 且若 $\int f = \rho e^{i\theta}$, 又若 h 由 $f = |f|e^{ih}$ 几乎处处有定义, 于是因为 $\mathrm{Re}(|f|(1 - e^{ih - i\theta}))$ 为正, 故有

$$\int |f| - |\int f| = \mathrm{Re}(\int |f| - |\int f|) = \mathrm{Re}(\int |f| - \int e^{-i\theta} f) = \mathrm{Re}(\int |f|(1 - e^{ih - i\theta})) \geqslant 0.$$

总之, 我们有 $|\int f| \leqslant \int |f|$.

(iii) 如果 $X \subset \mathbf{R}^m$ 可测, 且 $\phi \in \mathscr{L}^1(\mathbf{R}^m)$, 则由于 $|\mathbf{1}_X \phi| \leqslant |\phi|$, 有 $\mathbf{1}_X \phi \in \mathscr{L}^1(\mathbf{R}^m)$. 以 $\int_X \phi$ 记积分 $\int_{\mathbf{R}^m} \mathbf{1}_X \phi$, 其中 $\phi \in \mathscr{L}^1(\mathbf{R}^m)$.

5. 单调收敛和控制收敛定理 [306]

设 X 为 $\mathbf{R}^m$ 的可测子集. 称 $\phi : X \to \mathbf{C}$ 可测是说将 ϕ 以零值延拓到 $\mathbf{R}^m$ 得到的函数是可测的. 在 X 上可测的函数的集合 $\mathrm{Mes}(X)$ 因而自然地是 $\mathrm{Mes}(\mathbf{R}^m)$ 的一个子集, 从而定义 $\mathscr{L}^1(X)$ 为 $\mathrm{Mes}(X)$ 与 $\mathscr{L}^1(\mathbf{R}^m)$ 的交.

映射 $\phi \mapsto \mathbf{1}_X \phi$ 是 $\mathscr{L}^1(\mathbf{R}^m)$ 到它的子空间 $\mathscr{L}^1(X)$ 上的投射.

定理 III.1.30. — (单调收敛)

(i) 如果 $(f_n)_{n \in \mathbf{N}}$ 是 $\mathrm{Mes}(X, \overline{\mathbf{R}}_+)$ 中的一个递增序列, 则其极限可测, 并且 $\lim_{n \to +\infty} \int f_n = \int \lim_{n \to +\infty} f_n$.

(ii) 如果 $(u_n)_{n \in \mathbf{N}}$ 是 $\mathrm{Mes}(X, \overline{\mathbf{R}}_+)$ 中的序列, 则它们的级数和可测, 并且 $\int \sum_{n \in \mathbf{N}} u_n = \sum_{n \in \mathbf{N}} \int u_n$(对于在 $\mathbf{N} \times X$ 上的正函数的富比尼定理).

证明 (i) 直接可得 (考虑 $\mathbf{R}^m$ 上的一致收敛定理, 参看定理 III.1.18 的 (v)). (ii) 由将 (i) 用于部分和得到. □

命题 III.1.31. — (法图 (Fatou) 引理) 如果 $f_n \in \mathrm{Mes}(X, \overline{\mathbf{R}}_+)$, 则

$$\int (\liminf f_n) \leqslant \liminf \int f_n.$$

证明 令 $g_n = \inf_{k\geqslant n} f_k$. 于是, 作为可测函数单极限的 g_n 也可测, 并且根据下极限的定义知有递增的序列 $g_n \to \liminf f_n$. 按照单调收敛定理, 因此有 $\int g_n \to \int \liminf f_n$. 另外, 对于任意的 n, 成立 $\int g_n \leqslant \int f_n$. 因此有

$$\int \liminf f_n = \lim \int g_n = \liminf \int g_n \leqslant \liminf \int f_n,$$

这即所证. □

如果 $f \in \mathscr{L}^1(X)$, 我们定义它的 (半) 范数 $\|f\|_1$ 为 $\|f\|_1 = \int |f|$. 由定理 III.1.18 的 (iii) 得到, $\|f\|_1 = 0$ 当且仅当几乎处处 $f = 0$. 称 f_k 在 $\mathscr{L}^1(X)$ 趋向 f (或者 f_k 平均地趋向 f) 是说 $\|f_k - f\|_1 \to 0$. 由于 $\|f\|_1$ 是个半范数而非范数, 故一个序列的极限不是唯一的; 事实上如果在 $\mathscr{L}^1(X)$ 中有 $f_k \to f$, 则对于所有几乎处处满足 $g - f = 0$ 的 g 都在 $\mathscr{L}^1(X)$ 中有 $f_k \to g$.

由注记 III.1.29 的 (ii) 得到 $|\int f| \leqslant \|f\|_1$, 从而 $f \mapsto \int f$ 在 $\mathscr{L}^1(X)$ 中是连续的线性泛函 (甚至是 1-利普希茨的).

定理 III.1.32. — (控制收敛)

如果 $(f_n)_{n\in\mathbf{N}}$ 是 $\mathscr{L}^1(X)$ 中的序列, 它满足

- *存在 $g \in \mathscr{L}^1(X)$ 使得对任意的 $n \in \mathbf{N}$, 有 $|f_n| \leqslant g$ a.e. (控制函数),*
- *f_n 几乎处处单收敛, 则序列 $(f_n)_{n\in\mathbf{N}}$ 的几乎处处存在的极限 f 属于 $\mathscr{L}^1(X)$, 并且 f_n 在 $\mathscr{L}^1(X)$ 中趋向 f; 特别地, $\lim_{n\to+\infty} \int f_n \to \int f$.*

[307] 证明 由于 f 是可测函数的几乎处处的单极限故可测, 又由于 $|f| \leqslant g$ 几乎处处成立, 故 f 可和 (如果 $A_n = \{x, |f_n| > g\}$, 则当 $x \notin A = \cup_{n\in\mathbf{N}} A_n$ 时有 $|f| \leqslant g$; 由于 A_n 对所有的 n 为零测度集, 故 A 也为零测度集). 另外, 如有必要可在一个零测度集上改动 g 和这些 f_n, 从而可假设处处有 $|f_n| \leqslant g$. 因此有 $|f_n - f| \leqslant 2g$, 故可应用法图引理到 $h_n = 2g - |f_n - f|$ 上. 由于 $h_n \to 2g$, 所以有

$$\int 2g \leqslant \liminf \int 2g - |f_n - f| = \int 2g - \limsup \int |f_n - f|,$$

又由于 $\int 2g$ 有限, 故得到 $\limsup \int |f_n - f| \leqslant 0$, 但因 $\int |f_n - f| \geqslant 0$, 故对于任意的 $n \in \mathbf{N}$, $\int |f_n - f| \to 0$. 得到结论. □

习题 III.1.33. — 如果 $n \geqslant 1$, 令 $f_n = n\mathbf{1}_{[0,1/n]}$, $g_n = \frac{1}{n}\mathbf{1}_{[0,n]}$. 证明 $f_n \to 0$, $g_n \to 0$ *a.e.*, 并且 $\int f_n = \int g_n = 1$. 由此可推出 $1 = 0$ 吗?

习题 III.1.34. — (i) 证明 $\Gamma(s) = \int_0^{+\infty} e^{-t} t^{s-1} dt$ 对于 $s > 0$ 是有限的.

(ii) 证明当 $n \to \infty$ 时 $\lim_{n\to\infty} \int_0^n (1 - \frac{t}{n})^n t^{s-1} dt \to \Gamma(s)$.

(iii) 由此推出高斯公式 $\Gamma(s) = \lim_{n\to\infty} \frac{n! n^s}{s(s+1)\cdots(s+n)}$.

习题 III.1.35. — 设 $f : \mathbf{R}_+ \to \mathbf{R}_+$ 为递增和可和的. 证明 $\lim_{t\to+\infty} t f(t) = 0$.

习题 III.1.36. — 设 $f \in \mathscr{L}^1(\mathbf{R}^m)$, A_n 对所有 $n \in \mathbf{N}$ 是 $\mathbf{R}^m$ 的可测子集.

(i) 证明如果 A_n 递增且 $\cup_{n\in\mathbf{N}} A_n = \mathbf{R}^m$, 则 $\int_{\mathbf{R}^m} f = \lim_{n\to+\infty} \int_{A_n} f$.

(ii) 证明如果 $\lambda(A_n) \to 0$, 则 $\int_{A_n} f \to 0$. (利用博雷尔–坎泰利定理或者定理 III. 2.11.)

6. 主要的应用

后面的这个结果对于显式计算一维的积分非常有用, 而后面要讨论的富比尼定理将用于将对任意维数的积分计算化为一系列的对单变元被积函数的积分计算 (这样便可不必返回到定义上了!).

定理 III.1.37. — (分析的基本定理)

如果 $f : [a,b] \to \mathbf{C}$ 连续, 而 $F : [a,b] \to \mathbf{C}$ 可求导且导数为 f, 则 $\int_{[a,b]} f = F(b) - F(a)$.

证明 分别考虑 $\mathrm{Im}(F)$ 和 $\mathrm{Re}(F)$, 则由线性性化成了 F 为实函数的情形. 如果 $n \in \mathbf{N}$ 而 $i \in \{0, 1, \ldots, n\}$, 则令 $c_{n,i} = a + i\frac{b-a}{n}$, 而 $f_n : [a,b] \to \mathbf{R}$ 为对所有 $i \in \{0, \ldots, n-1\}$ 的 $[c_{n,i}, c_{n,i+1}[$ 上取值 $\frac{n}{b-a}(F(c_{n,i+1}) - F(c_{n,i}))$ 的函数. 于是对所有 n 有 $\int f_n = \sum_{i=0}^{n-1}(F(c_{n,i+1}) - F(c_{n,i})) = F(b) - F(a)$. 有限增量定理表明存在 $u_{n,i} \in [c_{n,i}, c_{n,i+1}[$ 使得当 $t \in [c_{n,i}, c_{n,i+1}[$ 时, $f_n(t) = f(u_{n,i})$, 从而 $f_n(t) = f(u_n(t))$, 其中 $|t - u_n(t)| \leqslant \frac{b-a}{n}$. 由此得到, 对于所有 n 有 $|f_n| \leqslant \|f\|_\infty$, 并且作为连续函数的 f, f_n 在 $[a,b]$ 上单趋向 f. 因此应用控制收敛定理得知, 极限与积分可交换, 这给出了 $\int_{[a,b[} f = F(b) - F(a)$. 注意到 $\{b\}$ 为零测度集, 便得到了 $\int_{[a,b[} f = \int_{[a,b]} f$, 便推出 [308] 结论. □

习题 III.1.38. — 设 $f : [a,b] \to \mathbf{C}$ 可导. 证明 f' 可测, 且若 f' 有界, 则 $\int_a^b f' = f(b) - f(a)$.

定理 III.1.39. — (对于级数的控制收敛定理)

设 I 是一个可数集, 而 $(a_{n,i})_{n\in\mathbf{N}, i\in I}$ 为满足以下条件的复数:

- *存在 $(b_i)_{i\in I}$, 满足 $\sum_{i\in I} |b_i| < +\infty$, 使得对于所有 $n \in \mathbf{N}$, $i \in I$ 有 $|a_{n,i}| \leqslant b_i$,*
- *对所有的 $i \in I$. $\lim_{n\to+\infty} a_{n,i}$ 存在.*

于是 $\lim_{n\to+\infty} \sum_{i\in I} a_{n,i} = \sum_{i\in I} \lim_{n\to+\infty} a_{n,i}$.

证明 不妨设 $I = \mathbf{N}$, 并将这些级数转换为与一个级数 $(u_n)_{n\in\mathbf{N}}$ 相伴的 "局部常值" 函数的积分, 其中的这个函数在 $[n, n+1[$ 上为 u_n 而在 $\mathbf{R}_-^*$ 上取值 0. 那么定理的断言可由定理 III.I.32 推出 (事实上, 麻烦一点也可直接证明, 参看小词典的 15.3 小节). □

III.2. 一些函数空间

1. 空间 $L^1(X)$

后文中, X 总代表 $\mathbf{R}^m$ 中的一个可测子集.

定理 III.2.1. — ($\mathbf{N}\times X$ 上的富比尼定理)

设 $(u_n)_{n\in\mathbf{N}}$ 是 $\mathscr{L}^1(X)$ 中的使得 $\sum_{n\in\mathbf{N}}\int|u_n|<+\infty$ 的序列, 则

(i) 级数 $\sum_{n\in\mathbf{N}}u_n(t)$ 几乎处处 (绝对) 收敛.

(ii) 如果 $g=\sum_{n\in\mathbf{N}}u_n$ a.e., 则 $g\in\mathscr{L}^1(X)$, 并且通项为 u_n 的级数在 $\mathscr{L}^1(X)$ 中收敛于 g; 特别地, $\int_X g=\sum_{n\in\mathbf{N}}\int_X u_n$.

证明 设 $h(t)=\sum_{n\in\mathbf{N}}|u_n(t)|$. 根据单调收敛定理有 $\int_X h=\sum_{n\in\mathbf{N}}\int|u_n|$, 而假设条件表明 $\int_X h<+\infty$. 命题 III.1.21 让我们由此得到 $A_1=\{t\in X,\sum_{n\in\mathbf{N}}|u_n(t)|=+\infty\}$ 是一个零测度集, 并且由于 A_1 也恰是那些使得级数 $\sum_{n\in\mathbf{N}}u_n(t)$ 不是绝对收敛的 $t\in X$ 的集合, 故得到 (i).

令 A_2 为那些使得 $g(t)\neq\sum_{n\in\mathbf{N}}u_n(t)$ 的 $t\in X$ 的集合. 于是由假设条件知 A_2 是一个零测度集, 因此 $A=A_1\cup A_2$ 作为两个零测度集的并仍是零测度的. 令 S 为如下定义的函数: 当 $t\notin A$ 时 $S(t)=\sum_{n\in\mathbf{N}}u_n(t)$, 而当 $t\in A$ 时 $S(t)=0$. 如果 $N\in\mathbf{N}$, 令 $S_N=\sum_{n\leqslant N}u_n$ 为此级数的部分和. 于是有 $S=g$ a.e., 那么为了证明第二个断言只要证明 S 是可和的并且 $\|S-S_N\|_1\to 0$ 即可. 然而, 对任意的 $t\notin A$ 和 $N\in\mathbf{N}$ 有 $|S_N(t)|\leqslant h(t)$, 从而对任意的 $t\notin A$ 有 $|S(t)|\leqslant h(t)$. 由此推出 S 可和. 又, 在 A 之 [309] 外有 $|S_N-S|\leqslant 2h$, 因此当 $t\notin A$ 时 $|S_N(t)-S(t)|\to 0$. 因为 A 是零测度的, 故它满足应用控制收敛的条件; 于是 $\int|S_N-S|\to 0$. 证完. □

习题 III.2.2. — 设 $f\in\mathscr{L}^1(\mathbf{R})$, $T\in\mathbf{R}_+^*$. 证明 $f_T(x)=\sum_{n\in\mathbf{Z}}f(x+nT)$ 几乎处处收敛并且 f_T 在 $[0,T]$ 上可和.

习题 III.2.3. — 定义 $f:\mathbf{R}\to\mathbf{R}_+$ 为: 当 $0<|x|<1$ 时 $f(x)=|x|^{-1/2}$, 而在其他点 $f(x)=0$.

(i) 证明 f 可和.

(ii) 设 $n\to r_n$ 为 $\mathbf{N}$ 到 $\mathbf{Q}$ 上的一个双射. 证明 $F(x)=\sum_{n=0}^{+\infty}(\frac{-1}{2})^n f(x-r_n)$ 几乎处处绝对收敛, 并且和 $F(x)$ 可和, 从而计算 $\int_{\mathbf{R}}F(x)dx$. F 的图像是什么?

推论 III.2.4. — 如果 $(f_n)_{n\in\mathbf{N}}$ 是 $\mathscr{L}^1(X)$ 中的元的序列, 并在 $\mathscr{L}^1(X)$ 中趋向 f, 则在 $(f_n)_{n\in\mathbf{N}}$ 中可抽出一个子序列, 使其收敛于 f a.e..

证明 从 $(f_n)_{n\in\mathbf{N}}$ 中抽出子序列 $(g_n)_{n\in\mathbf{N}}$, 使得 $\|f-g_n\|_1\leqslant 2^{-n}$, $n\in\mathbf{N}$. 令 $u_n=g_n-g_{n-1}$, $n\geqslant 1$ 而 $u_0=g_0$. 由于 $\|u_n\|_1\leqslant\|g_n-f\|_1+\|g_{n-1}-f\|_1\leqslant 2^{1-n}$, 于是 $\sum_{n\in\mathbf{N}}\|u_n\|_1<+\infty$. 根据定理 III.2.1, 级数 $\sum_{n\in\mathbf{N}}u_n(x)$ 在 $\mathscr{L}^1(X)$ 中几乎处处收敛,

从而几乎处处存在极限 $g \in \mathscr{L}^1(X)$, 于是 $g_n = \sum_{i=0}^n u_i$ 在 $\mathscr{L}^1(X)$ 中趋向 g. 由于在 $\mathscr{L}^1(X)$ 中 $g_n \to f$, 因此 $\|f-g\|_1 = 0$, 这表明 $f = g$ a.e., 而 g_n 趋向 f a.e.. 证完. □

习题 III.2.5. — 如果 $2^k \leqslant n < 2^{k+1}$, 而 f_n 是 $[\frac{n-2^k}{2^k}, \frac{n+1-2^k}{2^k}[$ 的特征函数. 证明在 $\mathscr{L}^1([0,1])$ 中 $f_n \to 0$, 但 $f_n(x)$ 在每点 $x \in [0,1]$ 都不趋向 0. 这个结果与上面的推论不矛盾吗?

具有半范数 $\| \|_1$ 的空间 $\mathscr{L}^1(X)$ 不是分离的: 因为相差一个几乎处处为零的两个函数的距离为 0. 以 $L^1(X)$ 记 $\mathscr{L}^1(X)$ 的分离化. 由于 $\|f\|_1 = 0$ 当且仅当 $f = 0$ a.e., 故 $L^1(X)$ 是 $\mathscr{L}^1(X)$ 对于几乎处处为 0 的函数的子空间 Npp 的商; 我们因此可以将 $L^1(X)$ 想象成为可和函数空间 $\mathscr{L}^1(X)$, 但其中两个几乎处处相等的函数被看成是相同的[20].

注记 III.2.6. — 因为 $\int(f-g) = 0$ 当且仅当 $f = g$ a.e., 故积分 $f \mapsto \int f$ 在 $L^1(X)$ 上确有定义. 另外, $f \mapsto \int f$ 由于在 $\mathscr{L}^1(X)$ 上是线性的, 故在 $L^1(X)$ 上也是, 又由于 $|\int f| \leqslant \int |f| = \|f\|_1$, 故连续.

定理 III.2.7. — 空间 $L^1(X)$ 是一个巴拿赫空间.

证明 已经知道了 $\| \|_1$ 是 $L^1(X)$ 上的一个范数; 因此只需证明 $L^1(X)$ 是完备的即可. [310] 为此, 要证明所有按范数收敛的级数均收敛, 但这正是定理 III.2.1 的内容. □

2. 空间 $L^2(X)$

如果 X 是 $\mathbf{R}^m$ 的一个可测子集, 以 $\mathscr{L}^2(X)$ 记平方可和的可测函数 $f: X \to \mathbf{C}$ 的集合 (即: 使得 $\int_X |f(t)|^2 dt < +\infty$ 的函数). 直接可知 $\mathscr{L}^2(X)$ 在乘以标量时稳定, 而稍加证明则可知它在加法下也稳定, 这来自不等式 $|a+b|^2 \leqslant 2|a|^2 + 2|b|^2$. $a, b \in \mathbf{C}$, 及由此得到的 $\int_X |f+g|^2 \leqslant (2\int_X |f|^2 + 2\int_X |g|^2)$, 其中 $f, g \in \mathrm{Mes}(X)$. 换而言之, $\mathscr{L}^2(X)$ 是一个向量空间.

现在, 由于 $|ab| \leqslant \frac{1}{2}(|a|^2 + |b|^2)$, $a, b \in \mathbf{C}$, 因此我们可以推出, 当 $f, g \in \mathscr{L}^2(X)$ 时有 $\bar{f}g \in \mathscr{L}^1(X)$, 这让我们可定义 $\langle f, g\rangle \in \mathbf{C}$ 为 $\langle f, g\rangle = \int_X \bar{f}g$. 映射 $\langle , \rangle$ 除了定义本身外它满足一个标量积的所有性质. 我们有

$$\langle f, f\rangle = 0 \Leftrightarrow \int_X |f(t)|^2 = 0 \Leftrightarrow f \in \mathrm{Npp}(X).$$

换句话说, 映射 $f \mapsto \|f\|_2 = \langle f, f\rangle^{1/2}$ 定义了 $\mathscr{L}^2(X)$ 上的一个希尔伯特半范数. 以 $L^2(X)$ 记其相伴的分离化空间; 按照上面所做的, 这是 $\mathscr{L}^2(X)$ 对于 $\mathrm{Npp}(X)$ 的商空间. 像 $L^1(X)$ 那样, 可将 $L^2(X)$ 考虑为平方可和函数的空间 $\mathscr{L}^2(X)$, 其中几乎处处

[20] 对 $L^1(X)$ 的这个想法大概是最易于使用的了; 但应该注意, 当将 $L^1(X)$ 的一个元已经确定几乎处处有定义时, 因为可以在一个零测度集上改动它的值, 故它在每个点并没有确定的值. 换句话说, 我们可以谈到看成是变量 x 的函数 $f(x)$(譬如可以谈在积分中的变量变换, 或者定义 $L^1(X)$ 中一个函数与一个有界函数的乘积) 而不是 $f(x_0)$.

相等的函数视为同一个函数. 由于 $\langle f, g\rangle = 0$ 当且仅当 f 或 g 几乎处处为 0, 故半双线性形式 $\langle , \rangle$ 转到商空间时诱导了 $L^2(X)$ 上的一个标量积. 可以将它作为一个定义.

定理 III.2.8. — (菲舍尔–里斯, 1907) 具有范数 $\| \|_2$ 的空间 $L^2(X)$ 是一个希尔伯特空间, 其中 $\|f\|_2 = (\int_X |f|^2)^{1/2}$.

证明 根据定理前面的讨论, 只要证明 $L^2(X)$ 是完备的. 为此, 只需证明一个按范数收敛的级数有一个极限即可. 这非常类似于定理 III.2.7 的证明, 我们将其放在下面的习题中. 称在 $L^2(X)$ 中的收敛性为二次平均收敛. □

习题 III.2.9. — 设 $(u_n)_{n\in\mathbf{N}}$ 为 $\mathscr{L}^2(X)$ 中的元的序列, 满足 $\sum_{n\in\mathbf{N}} \|u_n\|_2 < +\infty$, 并定义 $h : X \to \overline{\mathbf{R}}_+$ 为 $h(t) = (\sum_{n\in\mathbf{N}} |u_n(t)|)^2$.

(i) 证明 $\int_X h < +\infty$. 由此推出存在零测度集 $A \subset X$ 使得当 $t \in X - A$ 时, 级数 $\sum_{n\in\mathbf{N}} u_n(t)$ 绝对收敛.

(ii) 对于 $t \notin A$, 以 $S(t)$ 记级数 $\sum_{n\in\mathbf{N}} u_n(t)$ 的和, 并以在 A 中取 0 延拓 S; 又当 $N \in \mathbf{N}$ 时, 令 $S_N(t) = \sum_{n\leqslant N} u_n(t)$. 证明 $|S - S_N|^2$ 被 $4h$ 控制, 其中 $N \in \mathbf{N}$ 任意.

(iii) 证明 $S \in \mathscr{L}^2(X)$, 且在 $L^2(X)$ 中 $S_N \to S$.

(iv) 证明, 如果在 $\mathscr{L}^2(X)$ 中 $f_n \to f$, 那么可以从 $(f_n)_{n\in\mathbf{N}}$ 中抽出一个子序列, 它几乎处处趋向 f.

[311] 3. 在 L^1 和 L^2 中的收敛性

注记 III.2.10. — (i) 看不出空间 $L^1(X)$ 和 $L^2(X)$ 有任何事先存在的关系. 但是, 由于它们都是从 $\mathrm{Mes}(X)$ 的一个子集对于 $\mathrm{Npp}(X)$ 取商得到的, 故我们可以稍微滥用符号地以 $L^1(X) + L^2(X)$ (分别地, $L^1(X) \cap L^2(X)$) 表示 $\mathscr{L}^1(X) + \mathscr{L}^2(X)$ (分别地, $\mathscr{L}^1(X) \cap \mathscr{L}^2(X)$) 对于 $\mathrm{Npp}(X)$ 的商空间. 换而言之, 我们将 $L^1(X) + L^2(X)$ 中的元看成是一个同时为可和与平方可和的函数, 并允许差一个几乎处处为零的函数.

(ii) 在 $L^1(\mathbf{R}^m)$ 和 $L^2(\mathbf{R}^m)$ 之间没有任何包含关系, 但是, 如果 X 具有限测度, 则有 $L^2(X) \subset L^1(X)$. 事实上, 柯西–施瓦茨不等式表明, 当 f 在 X 上平方可和时, 则有

$$\int_X |f| \leqslant (\int 1)^{1/2} (\int_X |f|^2)^{1/2} < +\infty.$$

上面的这个不等式实际上证明了这个包含映射 $\iota : L^2(X) \subset L^1(X)$ 是连续的, 并且 $\|\iota\| \leqslant \lambda(X)^{1/2}$.

设 X 为 $\mathbf{R}^m$ 中的一个开集. 回忆一下, $\mathscr{C}_c(X), \mathscr{C}_c^k(X)$ 和 $\mathscr{C}_c^\infty(X)$ 分别代表了 X 上的具有紧支集的连续的 (分别地, $\mathscr{C}^k$ 类的, $\mathscr{C}^\infty$ 类的) 函数空间. 因为一个几乎处处为零的连续函数恒等于零, 那么 $\mathscr{L}^1(X)$ 到 $L^1(X)$ 的自然投射诱导了上面列出的那三个空间到 $L^1(X)$ 的一个单射, 这让我们可以将它们看作 $L^1(X)$ 的子空间. 同样的理由, $\mathrm{Esc}(X)$ 以自然的方式看成是 $L^1(X)$ 的子空间.

要了解 $L^1(X)$ 或 $L^2(X)$ 中的一般的元素是十分难的 (习题 III.2.3), 而下面的非常有用的结果让我们可以从简单的函数着手并利用连续性进行推理, 从而可以在 $L^1(X)$ 或 $L^2(X)$ 上处理一般情形下的结果 (参看定理 IV.2.7). 它也证明了我们可以定义 $L^1(X)$ 和 $L^2(X)$ 为 $\mathscr{C}_c(X)$(或 $\mathrm{Esc}(X)$) 在范数 $\|\ \|_1$ 和 $\|\ \|_2$ 下的完备化.

定理 III.2.11. — 如果 X 是 $\mathbf{R}^m$ 的一个开集, 且 E 是 $\mathrm{Esc}(X), \mathscr{C}_c(X), \mathscr{C}_c^k(X)$, $k \in \mathbf{N}$ 或者 $\mathscr{C}_c^\infty(X)$ 其中之一的空间, 则 E 在 $L^1(X)$ 和 $L^2(X)$ 中稠密. 进一步, 如果 $\phi \in L^1(X) \cap L^2(X)$, 则存在 E 中的一个收敛于 ϕ 的序列, 它既在 $L^1(X)$ 中也在 $L^2(X)$ 中.

证明 如果 D_n 是包含在 $X \cap ([-2^n, 2^n[^m)$ 中的大小为 2^{-n} 的互不相交的初等砌块的并, 则 X 是递增的铺砌 D_n, $n \in \mathbf{N}$ 的并. 令 F 是空间 $L^1(X), L^2(X)$ 或者 $L^1(X) \cap L^2(X)$ 之一, 并设 $\phi \in F$(在 $L^1(X) \cap L^2(X)$ 上赋予范数 $\sup(\|\ \|_1, \|\ \|_2)$). 如果 $n \in \mathbf{N}$, 令 ϕ_n 为在 $x \in D_n$ 且当 $|\phi(x)| \leqslant n$ 时取值 $\phi(x)$ 而当 $x \notin D_n$ 或 $|\phi(x)| > n$ 时取值 0 的函数. 于是对于任意的 $x \in X$ 有 $\phi_n(x) \to \phi(x)$, 又由于 $|\phi_n| \leqslant |\phi|$ 和 $|\phi_n^2| \leqslant |\phi^2|$, 故根据控制收敛定理, ϕ_n 在 F 中收敛于 ϕ. 因此对于 $j \in \mathbf{N}$ 可以找到 n_j 使得 $\|\phi - \phi_{n_j}\|_F \leqslant 2^{-j}$. 现在, 由于 ϕ_{n_j} 是一个具有有界支集的有界可测函数, 故存在 $f_j \in \mathrm{Esc}(D_{n_j})$ 使得 $\|f_j - \phi_{n_j}\|_F \leqslant 2^{-j}$. 因此 $\|f_j - \phi\|_F \leqslant 2^{1-j}$. 由此推出了 [312] $\mathrm{Esc}(X)$ 在 F 中的稠性, 这证明了对于 $E = \mathrm{Esc}(X)$ 情形下的定理. 其余的情形利用存在适当的 $\mathscr{C}^\infty$ 函数可得 (参看下面的习题). □

习题 III.2.12. — 定义函数 φ_0 为: 当 $x \leqslant 0$ 时 $\varphi_0(x) = 0$, 而当 $x > 0$ 时 $\varphi_0(x) = e^{-1/x}$; 它是 $\mathbf{R}$ 上的一个 $\mathscr{C}^\infty$ 函数 (φ_0 在 $\mathbf{R}_+^*$ 上的 n 阶导数具有形式 $e^{-1/x} P_n(\frac{1}{x})$, 其中 P_n 是一个多项式; 而在 0^+ 趋向 0. 这使我们可以与 φ_0 在 $\mathbf{R}_-^*$ 上的 n 阶导数进行黏合).

(i) 从 φ_0 出发可以逐次构造 $\mathbf{R}$ 上的 $\mathscr{C}^\infty$ 函数:

- $\varphi_1 : \mathbf{R} \to [0,1]$, 它在 $[0,1]$ 外为 0, 而 $\int_0^1 \varphi_1 = 1$;
- $\varphi_2 : \mathbf{R} \to [0,1]$, 当 $x \leqslant 0$ 时取值为 0, 而当 $x \geqslant 1$ 时取值为 1;
- $\phi_\varepsilon : \mathbf{R} \to [0,1]$, 其中 $\varepsilon \in]0, \frac{1}{2}[$, 它在 $[0,1]$ 外为 0, 而在 $[\varepsilon, 1-\varepsilon]$ 取值为 1.

(ii) 完成定理 III.2.11 的证明.

推论 III.2.13. — 如果对于任意的 $\varphi \in \mathscr{C}_c^\infty(X)$, $f \in L^1(X)$ 满足 $\int_X \varphi f = 0$, 则 $f = 0$.

证明 由定理 III.2.11 的证明得知, 如果 $g \in L^1(X)$ 有界, 则可找到 $\mathscr{C}_c^\infty(X)$ 中的序列 $(g_n)_{n\in\mathbf{N}}$, 它在 $L^1(X)$ 中趋向 g, 并且对于每个 n 满足 $\|g_n\|_\infty \leqslant \|g\|_\infty$. 又, 若有需要可抽出一个子序列, 故可假定 $g_n \to g$ a.e. (推论 III.2.4).

这个过程可特别应用于下面情形: 即 $Y \subset X$ 是一个具有限测度的开集, 而函数 g_Y 定义为: 当 $f(x) = 0$ 或 $x \notin Y$ 时 $g_Y(x) = 0$, 而当 $f(x) \neq 0$ 且 $x \in Y$

时 $g_Y(x) = \bar{f}(x)/|f(x)|$. 于是序列 $g_n f$ 几乎处处趋向 $\mathbf{1}_Y|f|$, 并且对所有的 n 被 $\|g_Y\|_\infty|f| = |f|$ 控制. 因此应用控制收敛定理的条件, 让我们证明了 $\int g_n f \to \int_Y |f|$. 对于所有 $\phi \in \mathscr{C}_c^\infty(X)$ 满足 $\int_X \phi f = 0$ 的假定给出了对所有的 Y 有 $\int_Y |f| = 0$, 故由单调收敛定理也有 $\int |f| = 0$. 证完. □

4. 不同类型的收敛性的比较

设 X 是 $\mathbf{R}^m$ 中的一个开集, 而 ϕ_n, $n \in \mathbf{N}$ 和 f 是从 X 到 $\mathbf{C}$ 的函数. 我们已经遇到过序列 $(\phi_n)_{n\in\mathbf{N}}$ 趋向 f 的几种收敛性的概念; 或许概述各种不同的收敛性之间的关联会多少有些好处.

- 一致的 $\phi_n \to f \Rightarrow$ 单的 $\phi_n \to f \Rightarrow$ 几乎处处单的 $\phi_n \to f$.
- 几乎处处单的 $\phi_n \to f$ 并且 $(\phi_n)_{n\in\mathbf{N}}$ 由一个可和函数 (分别地, 平方可和) 控制 $\Rightarrow$ 在 $L^1(X)$(分别地, 在 $L^2(X)$) 中 $\phi_n \to f$.
- 在 $L^1(X)$ 或在 $L^2(X)$ 中 $\phi_n \to f \Rightarrow$ 存在一个几乎处处趋向 f 的 $(\phi_n)_{n\in\mathbf{N}}$ 的子序列.
- 如果 $\lambda(X) < +\infty$, 则在 $L^2(X)$ 中 $\phi_n \to f \Rightarrow$ 在 $L^1(X)$ 中 $\phi_n \to f$.

作为这一小节的结尾我们给出一个后面要用到的小结果.

引理 III.2.14. — 设 X 是 $\mathbf{R}^m$ 的一个开集.

[313] (i) 设 $\phi \in L^1(X)$, $g \in \mathscr{C}(X)$. 如果在 $L^1(X)$ 中存在一个序列 $(\phi_j)_{j\in\mathbf{N}}$, 它在 $L^1(X)$ 中趋向 ϕ, 并使得 $\phi_j(x) \to g(x)$ a.e., 则 $g \in L^1(X)$, 并且 $g = \phi$ a.e.

(ii) 将 $L^1(X)$ 换作 $L^2(X)$ 有同样的结果.

证明　对这两种情形的证明完全一样. 如有必要抽出序列 $(\phi_n)_{n\in\mathbf{N}}$ 的一个子序, 故不妨设 (参看推论 III.2.4 和习题 III.2.9 的 (iv))$\phi_j(x) \to \phi(x)$ a.e., 故有结论. □

5. 空间 L^p

空间 $L^1(X)$ 与 $L^2(X)$ 属于一个巴拿赫空间族 $L^p(X), p \in [1, +\infty]$, 这是由里斯在 1910 年引进的, 是 $\mathrm{Mes}(X)$ 的子空间 $\mathscr{L}^p(X)$ 的分离化空间 (事实上, 在所有的情形中 $L^p(X)$ 都是 $\mathscr{L}^p(X)$ 对于 $\mathrm{Npp}(X)$ 的商空间). 空间 $\mathscr{L}^p(X)$ 的定义如下.

- 如果 $1 \leqslant p < +\infty$, 定义 $\mathscr{L}^p(X)$ 为 $\mathrm{Mes}(X)$ 中的满足 $|f|^p$ 为可和的函数 f 的子空间. 闵可夫斯基不等式 $(\int |f+g|^p)^{1/p} \leqslant (\int |f|^p)^{1/p} + (\int |g|^p)^{1/p}$ 让我们证明了 $\mathscr{L}^p(X)$ 是一个向量空间, 且 $f \mapsto \|f\|_p = (\int |f|^p)^{1/p}$ 是 $\mathscr{L}^p(X)$ 上的一个半范数.
- 如果 $p = +\infty$, 则定义 $\mathscr{L}^\infty(X)$ 为 $\mathrm{Mes}(X)$ 中那些本质有界的函数 f 的子空间, 就是说, 存在零测度集 $A \subset X$ 和 $M \in \mathbf{R}_+$ 使得对于任意的 $t \in X - A$ 有 $|f(t)| \leqslant M$ 的那些 f. 以 $\|f\|_\infty$ 表示 $|f|$ 的本质上确界, 就是说使得存在零测度集 $A \subset X$ 使得对于所有 $t \in X - A$ 满足 $|f(t)|| \leqslant M$ 的那些 M 的集合的下确界. 因此 $\|\ \|_\infty$ 是

$\mathscr{L}^\infty(X)$ 上的一个半范数.

如果 X 是 $\mathbf{R}^m$ 这样的一个开集, 且 $p < +\infty$, 则阶梯函数在 $L^p(X)$ 中稠密. 但在 $p = +\infty$ 的情形则不是如此, 阶梯函数集合在其中的闭包是那些在无限远趋向 0 的有界函数.

空间 $L^2(X)$ 作为希尔伯特空间按照里斯定理是自反的. 在一般情形, 称 $q \in [1, +\infty]$ 为 p 的共轭指数是说它满足 $1/p + 1/q = 1$. 赫尔德不等式 $\int |fg| \leqslant \|f\|_p \|g\|_q$ 表明, 如果 $g \in L^p(X)$, 则 $f \mapsto \int fg$ 定义了 L^p 上的一个连续线性形式 Λ_g, 并且有 $\|\Lambda_g\| \leqslant \|g\|_q (p = 1$ 或 $p = +\infty$ 是平凡的情形). 如果 $p \neq +\infty$, 可以证明 $g \mapsto \Lambda_g$ 实际上是从 $L^q(X)$ 到巴拿赫空间 $L^p(X)$ 的对偶的一个等距映射(21). 但是 $L^\infty(\mathbf{R}^m)$ 的对偶则严格地大于 $L^1(\mathbf{R}^m)$.

习题 III.2.15. — (i) 证明当 $X \subset \mathbf{R}^m$ 可测时, $L^1(X)$ 和 $L^2(X)$ 可分离.

(ii) 证明 $L^\infty(\mathbf{R}^m)$ 不可分离.

III.3. 重积分

1. 富比尼定理

有限和 $\sum_{j,k} a_{j,k}$ 的计算可以先对 j 然后再对 k 求和, 也可以先对 k 后对再 j 求和. 下面的富比尼定理说的是, 对于积分而言 (在全都为可和的条件下) 这也成立. [314]

引理 III.3.1. — (对阶梯函数的富比尼定理) 映射 $f \mapsto \int_{\mathbf{R}^n} f$(分别地, $f \mapsto \int_{\mathbf{R}^m} f$) 是从 $\mathrm{Esc}(\mathbf{R}^{n+m})$ 到 $\mathrm{Esc}(\mathbf{R}^m)$(分别地, $\mathrm{Esc}(R^n)$) 的一个线性映射, 并且有

$$\int_{\mathbf{R}^m} |\int_{\mathbf{R}^n} f| \leqslant \int_{\mathbf{R}^{n+m}} |f| \quad 和 \quad \int_{\mathbf{R}^n} |\int_{\mathbf{R}^m} f| \leqslant \int_{\mathbf{R}^{n+m}} |f|,$$

以及

$$\int_{\mathbf{R}^m} (\int_{\mathbf{R}^n} f) = \int_{\mathbf{R}^{n+m}} f = \int_{\mathbf{R}^n} (\int_{\mathbf{R}^m} f).$$

证明 线性性来自积分的线性性. 现设 $r \in \mathbf{N}$, $\boldsymbol{j} = (j_1, \ldots, j_n) \in \mathbf{Z}^n$ 以及 $\boldsymbol{k} = (k_1, \ldots, k_m) \in \mathbf{Z}^m$. 以 $(\boldsymbol{j}, \boldsymbol{k})$ 记 $(j_1, \ldots, j_n, k_1, \ldots, k_m) \in \mathbf{Z}^{n+m}$. 直接计算表明

$$\int_{\mathbf{R}^n} e_{r,(\boldsymbol{j},\boldsymbol{k})} = 2^{-rn} e_{r,\boldsymbol{k}}, \quad \int_{\mathbf{R}^m} e_{r,(\boldsymbol{j},\boldsymbol{k})} = 2^{-rm} e_{r,\boldsymbol{j}},$$

$$\int_{\mathbf{R}^m} (\int_{\mathbf{R}^n} e_{r,(\boldsymbol{j},\boldsymbol{k})}) = 2^{-rn} \int_{\mathbf{R}^m} e_{r,\boldsymbol{k}} = 2^{-r(n+m)} = \int_{R^{n+m}} e_{r,(\boldsymbol{j},\boldsymbol{k})} = \int_{\mathbf{R}^n} (\int_{\mathbf{R}^m} e_{r,(\boldsymbol{j},\boldsymbol{k})}).$$

结论来自 f 对于充分大的 r 的形如 $f = \sum_{(\boldsymbol{j},\boldsymbol{k})} a_{(\boldsymbol{j},\boldsymbol{k})} e_{r,(\boldsymbol{j},\boldsymbol{k})}$ 的分解 (这是个有限和). □

(21)注意, 如果 X 具有限测度, 则 $L^p(X)$ 构成了一个递降的巴拿赫空间族 (当 $p \geqslant p'$ 时有 $L^p(X) \subset L^{p'}(X)$), 于是它们的对偶 $L^q(X)$ 构成了一个递增族. 换而言之, 函数空间越小则它的对偶越大, 当我们考虑有限维空间的情形时这有点奇怪, 但施瓦兹由于将它引向到广义函数的构造上而获得了菲尔兹奖 (1950).

命题 III.3.2. — (在 L^1 中的富比尼定理) 存在唯一的从 $L^1(\mathbf{R}^{n+m})$ 到 $(L^1(\mathbf{R}^m)$ (分别地, $L^1(\mathbf{R}^n))$ 的连续线性映射 $f \mapsto \int_{\mathbf{R}^n} f$ (分别地, $f \mapsto \int_{\mathbf{R}^m} f$), 它在 $\mathrm{Esc}(\mathbf{R}^{n+m})$ 上与有相同写法的映射相同, 并有

$$\int_{\mathbf{R}^m}(\int_{\mathbf{R}^n} f) = \int_{\mathbf{R}^{n+m}} f = \int_{\mathbf{R}^n}(\int_{\mathbf{R}^m} f).$$

证明 如果赋予所有这些空间以范数 $\|\ \|_1$, 则根据引理 III.3.1, 线性映射 $\int_{\mathbf{R}^n}$: $\mathrm{Esc}(\mathbf{R}^{n+m}) \to L^1(\mathbf{R}^m)$ 是一致连续的 (事实上是 1-利普希茨的). 由于 $L^1(\mathbf{R}^m)$ 完备且 $\mathrm{Esc}(\mathbf{R}^{n+m})$ 在 $L^1(\mathbf{R}^{n+m})$ 中稠密, 故映射 $\int_{\mathbf{R}^n} : \mathrm{Esc}(\mathbf{R}^{n+m}) \to L^1(\mathbf{R}^m)$ 由连续性可延拓到 $L^1(\mathbf{R}^{n+m})$ 上. 同样地, $\int_{\mathbf{R}^m} : \mathrm{Esc}(\mathbf{R}^{n+m}) \to L^1(\mathbf{R}^n)$ 也由连续性延拓到 $L^1(\mathbf{R}^{n+m})$ 上. 最后, 这三个映射

$$f \mapsto \int_{\mathbf{R}^m}(\int_{\mathbf{R}^n} f),\ f \mapsto \int_{\mathbf{R}^{n+m}} f,\ f \mapsto \int_{\mathbf{R}^n}(\int_{\mathbf{R}^m} f)$$

均在 $L^1(\mathbf{R}^{n+m})$ 上连续, 并在整个 $\mathrm{Esc}(\mathbf{R}^{n+m})$ 上相同. 得到结论. □

我们可以把命题 III.3.2 当作下一个定理中 (i) 的更加具体的形式 (并且也更容易用来计算重积分).

[315] **定理 III.3.3.** — (富比尼)

(i) 如果 $f \in \mathscr{L}^1(R^{n+m})$, 则

- 对于几乎所有的 $y \in \mathbf{R}^m$ 有 $f(\cdot, y) \in \mathscr{L}^1(\mathbf{R}^n)$, 并且 $y \mapsto \int_{\mathbf{R}^n} f(x,y)dx \in \mathscr{L}^1(\mathbf{R}^m)$.
- 对于几乎所有的 $x \in \mathbf{R}^n$ 有 $f(x, \cdot) \in \mathscr{L}^1(\mathbf{R}^m)$, 并且 $x \mapsto \int_{\mathbf{R}^m} f(x,y)dy \in \mathscr{L}^1(\mathbf{R}^n)$, 以及

$$\int_{\mathbf{R}^m}(\int_{\mathbf{R}^n} f(x,y)dx)dy = \int_{\mathbf{R}^{n+m}} f(x,y)dxdy = \int_{\mathbf{R}^n}(\int_{\mathbf{R}^m} f(x,y)dy)dx.$$

(ii) 如果函数 $f : \mathbf{R}^{n+m} \to \overline{\mathbf{R}}_+$ 可测, 且取值在 $\overline{\mathbf{R}}_+$ 中, 则

$$y \mapsto \int_{\mathbf{R}^n} f(x,y)dx \quad 和 \quad x \mapsto \int_{\mathbf{R}^m} f(x,y)dy$$

可测, 并且

$$\int_{\mathbf{R}^m}(\int_{\mathbf{R}^n} f(x,y)dx)dy = \int_{\mathbf{R}^{n+m}} f(x,y)dxdy = \int_{\mathbf{R}^n}(\int_{\mathbf{R}^m} f(x,y)dy)dx.$$

注记 III.3.4. — (i) 如果 $X \subset \mathbf{R}^n$, $Y \subset \mathbf{R}^m$ 为可测集, 则 $X \times Y \subset \mathbf{R}^{n+m}$ 可测, 我们则有一个相似于上面的断言, 其中的 $\mathbf{R}^n$ 换作 X, 而 $\mathbf{R}^m$ 换作 Y, $\mathbf{R}^{n+m}$ 换作 $X \times Y$. 这只要将在 $\mathbf{R}^{n+m}$ 上的断言写成形如 $\int_{\mathbf{R}^{n+m}} \mathbf{1}_{X\times Y}\phi$ 的 $X \times Y$ 上的积分即可.

(ii) 在实际应用上, 我们在用 (i) 以交换变量来计算积分前, 先要用 (ii) 来证明 $|f|$ 可和.

(iii) 也可将 (i) 用作一个半存在性的定理: 它断言, 如果 $f(x,y)$ 可和, 则 $\int f(x,y)dx$ 对几乎所有的 y 均收敛, 而 $\int f(x,y)dy$ 对几乎所有的 x 均收敛; 但是却不能由此推导出对于特定的 x 或 y 上这些积分的收敛性.

证明 设 $(f_k)_{k\in\mathbf{N}}$ 是 $\mathrm{Esc}(\mathbf{R}^{n+m})$ 中的一个序列, 它在 $\mathscr{L}^1(\mathbf{R}^{n+m})$ 中趋向 f, 并使得 $\sum_{k\in\mathbf{N}}\|f_{k+1}-f_k\|_1<+\infty$. 由引理 III.3.11 知级数 $\sum_{k\in\mathbf{N}}\int_{\mathbf{R}^n}(f_{k+1}-f_k)$ 的项属于 $\mathrm{Esc}(\mathbf{R}^m)$, 并按范数在 $\mathscr{L}^1(\mathbf{R}^m)$ 中收敛, 以及如果以 $g\in\mathscr{L}^1(\mathbf{R}^m)$ 记此极限, 则 $\int_{\mathbf{R}^m}g=\int_{\mathbf{R}^{n+m}}f$. 因此问题在于证明, 对于在一个零测度集 B 之外的 y, 函数 $x\mapsto f(x,y)$ 属于 $\mathscr{L}^1(\mathbf{R}^n)$, 而 $g(y)=\int_{\mathbf{R}^n}f(x,y)dx$. 我们需要下面的引理.

引理 III.3.5. — 如果 $A\subset\mathbf{R}^{n+m}$ 的测度为 0, 则下面定义的集合 A_1 和 A_2 分别在 $\mathbf{R}^n$ 和 $\mathbf{R}^m$ 中测度为 0:

$$A_1=\{x\in\mathbf{R}^n, A\cap(\{x\}\times\mathbf{R}^m)\text{不是零测度集}\},$$
$$A_2=\{y\in\mathbf{R}^m, A\cap(\mathbf{R}^n\times\{y\})\text{不是零测度集}\}.$$

证明 由 (m 和 n 的) 对称性, 只需对 A_1 进行证明. 设 $\varepsilon>0$. 由于 A 测度为 0, 故可找到 $\mathbf{R}^n$ 中的一个铺砌的序列 $(D_k)_{k\in\mathbf{N}}$ 以及 $\mathbf{R}^m$ 中一个铺砌的序列 $(E_k)_{k\in\mathbf{N}}$, 使得 $A\subset\cup_{k\in\mathbf{N}}D_k\times E_k$, 而 $\sum_{k\in\mathbf{N}}\lambda(D_k)\lambda(E_k)\leqslant\varepsilon$. 如果 $r\in\mathbf{N}$, $j\in\mathbf{N}$, 令 $B_{\varepsilon,r,j}$ 为那些满足 $\sum_{k\leqslant j,x\in D_k}\lambda(E_k)>2^{-r}$ 的 $x\in\mathbf{R}^n$ 的集合; 这是 $\mathbf{R}^n$ 的一个铺砌, 并有 $2^{-r}\lambda(B_{\varepsilon,r,j})\leqslant\sum_{k\leqslant j}\lambda(D_k)\lambda(E_k)\leqslant\varepsilon$. 另外, 序列 $(B_{\varepsilon,r,j})_{j\in\mathbf{N}}$ 是一个有限铺砌的递增序列, 因此 $\lambda^+(\cup_{j\in\mathbf{N}}B_{\varepsilon,r,j})=\lim_{j\to+\infty}\lambda(B_{\varepsilon,r,j})\leqslant2^r\varepsilon$. 然而那些使得 $\lambda^+(A\cap(\{x\}\times\mathbf{R}^m))>2^{-r}$ 的 $x\in\mathbf{R}^n$ 的集合 B_r 包含在 $\cup_{j\in\mathbf{N}}B_{\varepsilon,r,j}$ 中, 其中 $\varepsilon>0$ 任意. 因为对于 $\varepsilon>0$, 外度量 $\leqslant2^r\varepsilon$, 故这是一个零测度集, 最后, $A_1=\cup_{r\in\mathbf{N}}B_r$ 作为可数个零测度集的并是零测度的. [316] □

回到富比尼定理的证明. 由于 $\sum_{k\in\mathbf{N}}\|f_{k+1}-f_k\|_1<+\infty$, 那么由定理 III.2.1 得到级数 $\sum_{k\in\mathbf{N}}f_{k+1}(x,y)-f_k(x,y)$ 在一个零测度集 A 之外的 (x,y) 绝对收敛于 $f(x,y)$. 另外, 根据引理 III.3.5, 存在一个 $\mathbf{R}^m$ 的零测度子集 B_1 使得, 如果 $y\notin B_1$ 则 $A\cap(\mathbf{R}^n\times\{y\})$, 是在 $\mathbf{R}^n$ 中的零测度集. 如果 $y\notin B_1$, 于是对于在一个零测度集外的 x 有 $f_k(x,y)\to f(x,y)$.

同样地, 由于 $\sum_{k\in\mathbf{N}}\int_{\mathbf{R}^n}(f_{k+1}-f_k)dx$ 在 $\mathscr{L}^1(\mathbf{R}^m)$ 中按范数收敛于 g, 故存在零测度集 $B_2\subset\mathbf{R}^m$ 使得当 $y\notin B_2$ 时有 $\int_{\mathbf{R}^n}f_k(x,y)dx\to g(y)$.

现在, 将对阶梯函数的富比尼定理用到 $u_k=|f_{k+1}-f_k|$ 上, 然后先后两次应用单调收敛定理, 得到

$$\begin{aligned}\sum_{k\in\mathbf{N}}\int_{\mathbf{R}^{n+m}}|u_k(x,y)|dxdy&=\sum_{k\in\mathbf{N}}\int_{\mathbf{R}^m}(\int_{\mathbf{R}^n}|u_k(x,y)|dx)dy\\&=\int_{\mathbf{R}^m}(\sum_{k\in\mathbf{N}}\int_{\mathbf{R}^n}|u_k(x,y)|dx)dy\end{aligned}$$

$$= \int_{\mathbf{R}^m} (\int_{\mathbf{R}^n} \sum_{k\in\mathbf{N}} |u_k(x,y)|dx)dy.$$

由于有假设条件 $\sum_{k\in\mathbf{N}} \int_{\mathbf{R}^{n+m}} |u_k(x,y)|dxdy<+\infty$, 故那些使得 $\int_{\mathbf{R}^n} \sum_{k\in\mathbf{N}} |u_k(x,y)|dx = +\infty$ 的 $y \in \mathbf{R}^m$ 的集合 B_3 具零测度. 如果 $y \notin B_3$, 则函数 $h_y(x) = \sum_{k\in\mathbf{N}} |u_k(x,y)|$ 可和, 又因为 $f_k = \sum_{j=0}^{k-1} u_k$, 故有 $|f_k(x,y)| \leqslant h_y(x)$, 其中 $k \in \mathbf{N}$ 任意.

如果 $B = B_1 \cup B_2 \cup B_3$, 且 $y \notin B$, 则满足控制收敛的条件, 应用它便得到

$$g(y) = \lim_{k\to+\infty} \int_{\mathbf{R}^n} f_k(x,y)dx = \int_{\mathbf{R}^n} (\lim_{k\to+\infty} f_k(x,y))dx = \int_{\mathbf{R}^n} f(x,y)dx.$$

完成了对于 (i) 的证明.

除了 $\int_{\mathbf{R}^{n+m}} f(x,y)dxdy = +\infty$ 外, (ii) 是 (i) 的推论. 但在这种情形, 只要取一个 $\mathscr{L}^1(\mathbf{R}^{n+m})$ 中的序列 $(f_k)_{k\in\mathbf{N}}$, 它递增地趋向 f, 再考察以递增方式依赖 f 的这个恒等式的三项, 并利用单调收敛定理证明 $\lim_{k\to+\infty} \int_{\mathbf{R}^{n+m}} f_k(x,y)dxdy = +\infty$, 因此由此得到这三项都等于 $+\infty$. 证完. □

习题 III.3.6. — 定义 $f: \mathbf{R}_+ \times \mathbf{R}_+ \to \mathbf{R}$ 为: 当 $x \leqslant y$ 时 $f(x,y) = e^{x-y}$, 而当 $y < x$ 时 $f(x,y) = -e^{y-x}$. 计算

$$\int_0^{+\infty} (\int_0^{+\infty} f(x,y)dx)dy$$

和

$$\int_0^{+\infty} (\int_0^{+\infty} f(x,y)dy)dx.$$

由此能推出 $-1 = 1$ 吗?

习题 III.3.7. — (i) 设 $P \in \mathbf{R}[X,Y]$ 非零. 证明 $X = \{(x,y) \in \mathbf{R}^2, P(x,y) = 0\}$ 是 $\mathbf{R}^2$ 的零测度集. (注意 $\int_{\mathbf{R}^2} \mathbf{1}_X$.)

(ii) 设 $P \in \mathbf{R}[X_1,\dots,X_m]$ 非零. 证明 $\{x \in \mathbf{R}^m, P(x) = 0\}$ 是 $\mathbf{R}^m$ 中的零测度集.

[317] 2. 变量变换公式

定理 III.3.8. — (勒贝格测度的平移下的不变性)

如果 $v \in \mathbf{R}^m$ 及 $\phi: \mathbf{R}^m \to \mathbf{C}$ 可测, 则 $x \mapsto \phi(x+v)$ 可测, 并有

$$\int |\phi(x+v)|dx = \int |\phi(x)|dx \quad \text{并且, 如果 } \phi \text{ 可和, 则} \quad \int \phi(x+v)dx = \int \phi(x)dx.$$

证明　以 T_v 代表映射 $\phi \mapsto T_v(\phi)$, 其定义为 $(T_v(\phi))(x) = \phi(x+v)$. 如果 D 是一个砌块, 并且 v 的坐标已用 2 进位表示, 则 $D - v = \{x - v, x \in D\}$ 仍然是一个砌块, 而且有 $T_v(\mathbf{1}_D) = \mathbf{1}_{D-v}$; 将 D 和 $D - v$ 分割为具相同大小的初等砌块, 则因此有

$\int T_v(\mathbf{1}_D) = \int \mathbf{1}_D$. 在一般情形, 取 $\mathbf{R}^m$ 中的元的一个序列 $(v_n)_{n\in\mathbf{N}}$, 其中的 v_n 以二进位表示, 并且趋向位移 v: 序列 $\mathbf{1}_{D-v_n}$ 除了在各个面上以外简单地趋向 $\mathbf{1}_{D-v_n}$, 但这些面是零测度集 (例如, 见习题 III.1.6 的 (ii)), 这证明了 $\mathbf{1}_{D-v}$ 作为可测函数的几乎处处的单极限仍为可测函数, 从而可以应用控制收敛定理得到 $\int T_v(\mathbf{1}_D) = \int \mathbf{1}_D$.

由线性性得到 $T_v(\phi)$ 可测且 $\int T_v(\phi) = \int \phi$, 其中 $\phi \in \mathrm{Esc}(\mathbf{R}^m)$. 应用 $\mathrm{Esc}(\mathbf{R}^m)$ 在 $L^1(\mathbf{R}^m)$ 中的稠密性 (以及在处理 $\int |\phi| = +\infty$ 时的单调收敛定理), 便由此得到了定理. □

设 Ω 为 $\mathbf{R}^m$ 的一个开集, 且 $\varphi : \Omega \to \varphi(\Omega)$ 是 Ω 到 $\mathbf{R}^m$ 的一个开集 $\varphi(\Omega)$ 上的微分同胚, 就是说, 这是一个 $\mathscr{C}^1$ 类的双射, 而其逆也是 $\mathscr{C}^1$ 类的. 在坐标下, 映射 φ 可写为

$$\varphi(x) = (\varphi_1(x_1, \ldots, x_m), \ldots, \varphi_m(x_1, \ldots, x_m)),$$

"φ 是 $\mathscr{C}^1$ 类的" 等于说偏导数 $\frac{\partial \varphi_i}{\partial x_j}$ 在 Ω 上连续. 以 $\mathrm{Jac}_\varphi(x) = (\frac{\partial \varphi_i}{\partial x_j}(x))_{1\leqslant i,j\leqslant m}$ 为 φ 在点 x 的雅可比矩阵. 定义 φ 在 x 的雅可比 $J_\varphi(x)$ 为 $\mathrm{Jac}_\varphi(x)$ 的行列式; φ 为微分同胚意味着 $\mathrm{Jac}_\varphi(x)$ 可逆, 从而 $J_\varphi(x) \neq 0$, $x \in \Omega$.

定理 III.3.9. — 如果 f 是 $\varphi(\Omega)$ 上的一个可测函数, 则 f 可和当且仅当函数 $x \mapsto f(\varphi(x)) \cdot J_\varphi(x)$ 在 Ω 上可和; 并且成立

$$\int_{\varphi(\Omega)} f(y)dy = \int_\Omega f(\varphi(x)) \cdot |J_\varphi(x)| dx.$$

注记 III.3.10. — (i) 在一维的情形, φ 的雅可比矩阵就是 φ 的导数 φ', 于是公式化为 $\int_{\varphi(]a,b[)} f(y)dy = \int_{]a,b[} f(\varphi(x))|\varphi'(x)|dx$. 因为 φ' 在 $]a,b[$ 上不为零, 故有两种情形: 如果在 $]a,b[$ 上 $\varphi' > 0$, 则 $\varphi(]a,b[) =]\varphi(a), \varphi(b)[$, 如果在 $]a,b[$ 上 $\varphi' < 0$, 则 $\varphi(]a,b[) =]\varphi(b), \varphi(a)[$. 在第一种情形中该公式成为 $\int_{\varphi(a)}^{\varphi(b)} f(y)dy = \int_a^b f(\varphi(x))\varphi'(x)dx$, 而在第二种情形中, 则成为 $-\int_{\varphi(a)}^{\varphi(b)} f(y)dy = -\int_a^b f(\varphi(x))\varphi'(x)dx$. 在这两种情形我们都回 [318] 到了经典的公式.

(ii) 将变量变换公式写成一个非常实用的方式是将体积元 dx 和 dy 形式地显式表达为 $dx = |dx_1 \wedge \cdots \wedge dx_m|$ 和 $dy = |dy_1 \wedge \cdots \wedge dy_m|$. 由于 $y_i = \varphi_i(x)$, 故 $dy_i = \sum_{j=1}^m \frac{\partial \varphi_i}{\partial x_j}(x)dx_j$. 因为 $\wedge$ 是个交错乘积, 故有 $\wedge_{i=1}^m (\sum_{j=1}^m a_{i,j}dx_j) = \det(a_{i,j}) \wedge_{j=1}^m dx_j$ (这是定义 m 个向量的行列式的一种方式), 它给出了

$$dy = |\wedge_{j=1}^m (\sum_{j=1}^m \frac{\partial \varphi_i}{\partial x_j}(x)dx_j)| = |J_\varphi(x)dx_1 \wedge \cdots \wedge dx_m| = |J_\varphi(x)|dx.$$

证明　首先我们注意到问题可化到 $\Omega = \mathbf{R}^m$ 以及 φ 为仿射 (即具有形式 $x \mapsto A \cdot x + b$, 其中 $A \in \mathbf{GL}_m(\mathbf{R}^m)$, $b \in \mathbf{R}$) 的情形. 在这种情形下, φ 的雅可比矩阵为等于 A 的常值矩阵; 于是对于所有的 x 有 $J_\varphi(x) = |\det A|$.

另外, 如果 $r \in \mathbf{N}$, $\boldsymbol{k} \in \mathbf{Z}^m$, 则 $\varphi(D_{r,\boldsymbol{k}})$ 是一个 $\varphi(D_{r,\mathbf{0}})$ 的位移, 从而具有相同的体积. 由此推出存在 $C(A) \in \mathbf{R}_+^*$ 使得 $\lambda(\varphi(D_{r,\boldsymbol{k}})) = 2^{-r}C(A)$, 其中 $r \in \mathbf{N}$, $\boldsymbol{k} \in \mathbf{Z}^m$

任意. 由线性性, 对于 $\phi \in \mathrm{Esc}(\mathbf{R}^m)$ 便有 $\int_{\mathbf{R}^m}\phi(x)dx = C(A)\int_{\mathbf{R}^m}\phi(A\cdot x+b)dx$. 再由连续性, 这个等式可延拓到 $L^1(\mathbf{R}^m)$ 上. 要证明断言在仿射情形成立还需证明 $C(A) = |\det A|$, 它构成了行列式的几何解释[22], 是后面习题 III.3.11 的内容.

对于一般情形的证明我们将利用如下事实, 即越靠近 x 观察映射 φ, 它就越像仿射映射 $h \mapsto \varphi(x) + \mathrm{Jac}_\varphi(x)\cdot h$, 从而当 r 趋向 $+\infty$ 时, $x + D_{r,\mathbf{0}}$ 的像就越来越像超平行体 $\varphi(x) + \mathrm{Jac}_\varphi(x)\cdot D_{r,\mathbf{0}}$, 因而其体积为 $|J_\varphi(x)|\lambda(D_{r,\mathbf{0}})$. □

「 更准确地, 我们可利用当 $K \subset \Omega$ 为紧集时 $x \mapsto \mathrm{Jac}_\varphi(x)$(和 $x \mapsto \mathrm{Jac}_{\varphi^{-1}}(x)$) 的一致连续性来进行证明. 这时存在一个函数序列 $\varepsilon_{K,r} : K \to \mathbf{R}_+$, 其中 r 充分大, 它在 K 上一致地趋向 0, 并使得对于任意的 $x \in K$ 有

$$\varphi(x) + (1-\varepsilon_{K,r}(x))\mathrm{Jac}_\varphi(x)\cdot D_{r,\mathbf{0}} \subset \varphi(x + D_{r,\mathbf{0}}) \subset \varphi(x) + (1+\varepsilon_{K,r}(x))\mathrm{Jac}_\varphi(x)\cdot D_{r,\mathbf{0}}.$$

由此推出在 K 上一致趋向 0 的序列 $\varepsilon'_{K,r}$, 使得对任意的 $x \in K$ 有 $\lambda(\varphi(x + D_{r,\mathbf{0}}) = (1+\varepsilon'_{K,r}(x))|J_{\varphi(x)}|\lambda(x + D_{r,\mathbf{0}})$. 现在, 可以将 Ω 写为递增的铺砌 D_n 的并, 而且这些铺砌的闭包仍包含在 Ω 内, 于是只要证明定理中的公式对于一个支集在某个 D_n 中的阶梯函数 f 成立即可: 因为这些函数构成了 $\mathscr{L}^1(\Omega)$ 中一个稠密的子空间. 由线性性, 于是问题化为证明 $\lambda(\varphi(D)) = \int_D |J_\varphi|dx$, 其中 D 是闭包 K 在 Ω 内的初等砌块. 如果 r 充分大, 则 D 是包含在 D 中的不交 $D_{r,\boldsymbol{k}}$ 的并, 而由于 $D_{r,\boldsymbol{k}} = \frac{\boldsymbol{k}}{2^r} + D_{r,\mathbf{0}}$, 那么从上面的讨论中得知

$$\begin{aligned}\lambda(\varphi(D)) &= \sum_{D_{r,\boldsymbol{k}}\subset D}\lambda(\varphi(\frac{\boldsymbol{k}}{2^r} + D_{r,\mathbf{0}})) = \sum_{D_{r,\boldsymbol{k}}\subset D}(1+\varepsilon'_{K,r}(\frac{\boldsymbol{k}}{2^r}))|J_\varphi(\frac{\boldsymbol{k}}{2^r})|\lambda(D_{r,\boldsymbol{k}})\\ &= \int_D \phi_r(x)dx,\end{aligned}$$

其中 ϕ_r 是 D 上的阶梯函数, 它在 $D_{r,\boldsymbol{k}}$ 上取值 $(1+\varepsilon'_{K,r}(\frac{\boldsymbol{k}}{2^r}))|J_\varphi(\frac{\boldsymbol{k}}{2^r})|$. 由于 $\varepsilon'_{K,r}$ 在 K 上一致地趋向 0, 故 ϕ_r 在 D 上一致地趋向 $|J_\varphi(x)|$. 得到了结果. 」

[319] **习题 III.3.11.** — (i) 证明对于任意的 $A, B \in \mathbf{GL}_m(\mathbf{R})$ 有 $C(AB) = C(A)C(B)$.

(ii) 证明如果 A 是个对角矩阵或一个置换矩阵 (即 $x \mapsto A\cdot x$ 诱导了 $\mathbf{R}^m$ 的标准基向量间的置换), 则 $C(A) = |\det A|$.

(iii) 证明所有的幂幺上三角或下三角矩阵 (即对角线元为 1 的上或下三角矩阵) 可以写成 $DUD^{-1}U^{-1}$ 的形式, 其中 D 为对角矩阵, 而 U 为幂幺上三角或下三角矩阵. 由此推出当 A 为幂幺上三角或下三角矩阵时 $C(A) = 1$.

(iv) 利用高斯消元法证明 $\mathbf{GL}_m(\mathbf{R})$ 由对角矩阵, 幂幺上三角或下三角矩阵和置换矩阵生成.

(v) 推导出, 对任意的 $A \in \mathbf{GL}_m(\mathbf{R})$ 有 $C(A) = |\det A|$.

---

[22] $\mathbf{R}^m$ 中的向量 $v_1, \ldots, v_m$ 张成的超平行体的体积等于这些向量的行列式的绝对值.

3. 高斯积分

我们将利用前两小节的结果建立公式

$$\int_{-\infty}^{+\infty} e^{-x^2} dx = \sqrt{\pi} \quad 和 \quad \int_{-\infty}^{+\infty} e^{-\pi x^2} dx = 1.$$

用变量变换 $x = \sqrt{\pi} u$ 可将第一个公式化为第二个, 故只需证明第一个就可以了. 为此, 将要计算的积分记为 $I = \int_{-\infty}^{+\infty} e^{-x^2} dx$, 并令 $I_0 = \int_{\mathbf{R}^2} e^{-(x^2+y^2)} dxdy$.

- 由 $e^{-(x^2+y^2)} = e^{-x^2} e^{-y^2}$, 并根据对于正函数的富比尼定理得到

$$I_0 = \int_{\mathbf{R}} (\int_{\mathbf{R}} e^{-x^2} e^{-y^2} dx) dy = \int_{\mathbf{R}} I e^{-y^2} dy = I^2.$$

- 令 Δ 为半直线 $]-\infty, 0] \times \{0\}$ 和 $\Omega' = \mathbf{R}^2 - \Delta$, 由于 Δ 的测度为 0, 故 $I_0 = \int_{\Omega'} e^{-(x^2+y^2)} dxdy$.
- 令 $\Omega = \mathbf{R}_+^* \times]-\pi, \pi[$. 于是由 $\varphi(r, \theta) = (r\cos\theta, r\sin\theta)$ 定义的 φ 是 Ω 到 Ω' 的微分同胚, 并由于 $dx = \cos\theta dr - r\sin\theta d\theta$ 和 $dy = \sin\theta dr + r\cos\theta d\theta$, 那么 φ 的雅可比矩阵为 $\begin{pmatrix} \cos\theta & -r\sin\theta \\ \sin\theta & r\cos\theta \end{pmatrix}$, 从而其雅可比为 $J_\varphi(r, \theta) = r\cos^2\theta + r\sin^2\theta = r$. 将变量变换公式用于函数 $f(x, y) = e^{-(x^2+y^2)}$ 则给出

$$I_0 = \int_\Omega e^{-(r^2\cos^2\theta + r^2\sin^2\theta)} |J_\varphi(r, \theta)| dr d\theta = \int_\Omega e^{-r^2} r dr d\theta.$$

- 再用对于正函数的富比尼定理:

$$I_0 = \int_{\mathbf{R}_+^* \times]-\pi, \pi[} e^{-r^2} r dr d\theta = \int_0^{+\infty} (\int_{-\pi}^{+\pi} e^{-r^2} r d\theta) dr = 2\pi \int_0^{+\infty} e^{-r^2} r dr.$$

- 最后, 变量变换 $r^2 = u$, 因而 $rdr = \frac{1}{2} du$ 给出

$$I_0 = \pi \int_0^{+\infty} e^{-u} du = \pi[-e^{-u}]_0^{+\infty} = \pi.$$

由于 $I_0 = I^2$ 便得结论.

4. 习题

[320]

习题 III.3.12. — (两个可和函数的卷积) 设 $f, g \in \mathscr{L}^1(\mathbf{R}^m)$.

(i) 证明 $\int\int |f(x-y)g(y)| = \|f\|_1 \|g\|_1$.

(ii) 由此推导出, 对几乎所有的 x 函数 $y \mapsto f(x-y)g(y)$ 可和, 并且由 $f * g(x) = \int f(x-y)g(y) dy$ a.e. 定义的 $f * g$ 也是可和的.

(iii) 证明, 如果 $f_1 = f_2$ a.e., $g_1 = g_2$ a.e., 则 $f_1 * g_1 = f_2 * g_2$ a.e. (映射 $(f,g) \mapsto f * g$ 转到商时便定义了从 $L^1(\mathbf{R}^m) \times L^1(\mathbf{R}^m)$ 到 $L^1(\mathbf{R}^m)$ 的一个映射, 我们仍记其为 $(f,g) \mapsto f * g$.)

(iv) 证明 $(f,g) \mapsto f * g$ 诱导了从 $L^1(\mathbf{R}^m) \times L^1(\mathbf{R}^m)$ 到 $L^1(\mathbf{R}^m)$ 的一个连续的双线性映射, 并有 $f * g = g * f$ 和 $f * (g * h) = (f * g) * h$, 其中 $f, g, h \in L^1(\mathbf{R}^m)$.

习题 III.3.13. — 设 ϕ 是 $\mathbf{R}^m$ 上的一个 $\mathscr{C}^\infty$ 函数, 其支集含在 $[-1,1]^m$ 中, 而取值于 $\mathbf{R}_+$ 中, 并满足 $\int_{\mathbf{R}^m} \phi = 1$. 如果 $\varepsilon > 0$, 令 $\phi_\varepsilon(x) = \varepsilon^{-m}\phi(\frac{x}{\varepsilon})$.

(i) 证明 $\int_{\mathbf{R}^m} \phi_\varepsilon = 1$, 并且 ϕ_ε 的支集含在 $[-\varepsilon, \varepsilon]^m$ 之中.

(ii) 证明, 如果 f 是一个阶梯函数, 则当 $\varepsilon \to 0$ 时, 有 $f * \phi_\varepsilon \to f$ a.e.

(iii) 证明, 如果 f 是一个阶梯函数, 则当 $\varepsilon \to 0$ 时, 在 $L^1(\mathbf{R}^m)$ 中有 $f * \phi_\varepsilon \to f$.

(iv) 证明, 如果 $f \in L^1(\mathbf{R}^m)$, 则在 $L^1(\mathbf{R}^m)$ 中, 当 $\varepsilon \to 0$ 时 $f * \phi_\varepsilon \to f$.

(v) 证明, 如果 $f \in L^1(\mathbf{R}^m) + L^2(\mathbf{R}^m)$ 对于所有的 $\phi \in \mathscr{C}_c^\infty(\mathbf{R}^m)$ 满足 $\int_{\mathbf{R}^m} \phi f = 0$, 则 $f = 0$ a.e.

习题 III.3.14. — 设 $f, g \in L^2(\mathbf{R}^n)$.

(i) 证明 $\|f * g\|_\infty \leqslant \|f\|_2 \|g\|_2$.

(ii) 证明 $f * g$ 连续并在无限远处趋向 0 (从阶梯函数着手).

(iii) 证明, 如果 A 和 B 是 $\mathbf{R}^n$ 中的两个具严格正测度的子集, 则集合 $A + B = \{a + b, a \in A, b \in B\}$ 包含了一个开集.

(iv) 内核为空的闭集是否必为零测度集?

习题 III.3.15. — (i) 建立公式 $\int_0^1 \int_0^1 \frac{dxdy}{1-x^2y^2} = \frac{3}{4}\zeta(2)$.

(ii) 设 $\Omega_1 = \{(u,v), u > 0, v > 0, u + v < \frac{\pi}{2}\}$ 和 $\Omega_2 = \{(x,y), 0 < x, y < 1\}$. 证明定义为 $\varphi(u,v) = (\frac{\sin u}{\cos v}, \frac{\sin v}{\cos u})$ 的 ϕ 诱导了从 Ω_1 到 Ω_2 的一个微分同胚.

(iii) 由此得出 $\zeta(2) = \frac{\pi^2}{6}$.

习题 III.3.16. — 设 $N \in \mathbf{N} - \{0\}$, 而 $\varphi : \mathbf{R}^2 \to \mathbf{R}^2$ 是由 $\mathbf{C} \to \mathbf{C} : z \mapsto z^N$ 将 $\mathbf{C}$ 等同于 $\mathbf{R}^2$ 时所诱导的映射. φ 在 $z_0 \in \mathbf{C}$ 的雅可比是 $|Nz_0^{N-1}|^2$(参看注记 V.3.1 的 (i)). 证明, 如果 f 在 $\mathbf{R}^2$ 上可和, 则

$$\int_{\mathbf{R}^2} f(u,v)dudv = N \int_{\mathbf{R}^2} f(\varphi(u,v))(x^2+y^2)^{N-1}dxdy.$$

习题 III.3.17. — ($\mathbf{R}^m$ 中单位球的体积)[23]

设 $m \geqslant 1$. 赋予 $\mathbf{R}^m$ 以标准的欧几里得范数 $\|\ \|$. 如果 $B(\rho)$ ($\rho \in \mathbf{R}_+$) 为中心为 0 半径为 ρ 的球. 以 C_m 记 $B(1)$ 的体积.

(i) 证明 $\lambda(B(\rho)) = C_m \rho^m$.

---

[23]对于 $n = 3$ 的结果已在 1150 年左右为印度数学家 Bhaskaracarya 所知.

(ii) 设 $\phi_r = \sum_{k=1}^{2^r}(\frac{k}{2^r})^{1-m}\mathbf{1}_{B(\frac{k}{2^r})-B(\frac{k-1}{2^r})}$. 证明 $\int_{\mathbf{R}^m}\phi_r \to \int_{B(1)}\|x\|^{1-m}dx$.

(iii) 由此推出 $\int_{B(1)}\|x\|^{1-m}dx = mC_m$.

(iv) 证明, 如果 $\phi \in \mathrm{Esc}(\mathbf{R}_+)$, 则 $mC_m\int_{\mathbf{R}_+}\phi(t)dt = \int_{\mathbf{R}^m}\|x\|^{1-m}\phi(\|x\|)dx$. 由此推出 $\phi \in L^1(\mathbf{R}_+)$ 当且仅当 $\|x\|^{1-m}\phi(\|x\|) \in L^1(\mathbf{R}^m)$, 并且 $mC_m\int_{\mathbf{R}_+}\phi(t)dt = \int_{\mathbf{R}^m}\|x\|^{1-m}\phi(\|x\|)dx$, 其中 $\phi \in L^1(\mathbf{R}_+)$ 任意.

(v) 设 $s \in \mathbf{R}$. 证明 $\int_{\|x\|\leqslant 1}\|x\|^s < +\infty$ 当且仅当 $s > -m$, 以及 $\int_{\|x\|\geqslant 1}\|x\|^s < +\infty$ 当且仅当 $s < -m$. [321]

(vi) 应用前面结果于函数 $t^{m-1}e^{-\pi t^2}$, 并利用 $\pi = C_2$ 的定义, 推导出 $\int_{\mathbf{R}} e^{-\pi x^2}dx$ 的结果, 并证明 $C_m = \frac{\pi^{m/2}}{\Gamma(1+\frac{m}{2})}$.

III.4. 勒贝格积分的构造

这一节致力于证明定理 III.1.18 和 III.1.23 以及命题 III.1.12, 它们是整个理论的基础. 首先我们注意到, 在从定理 III.1.18 推导控制收敛定理时没有用到唯一性. 如果能够定义积分的话, 那么由此便知以下的结果应该成立.

命题 III.4.1. — *设 D 是一个铺砌, 而 $M > 0$. 并设 $h \in \mathrm{Mes}(D,[0,M])$, 且 $(h_n)_{n\in\mathbf{N}}$ 是一个 $\mathrm{Esc}(D,[0,M])$ 中的元的序列, 它几乎处处趋向 h. 于是 $\int h_n$ 有一个只与 h 有关的极限.*

进一步说, 如果这个结果成立, 则控制收敛定理和单调收敛定理表明我们应该按照下面的方式定义勒贝格积分[24].

(L1) 如果 $f \in \mathrm{Mes}(D,[0,M])$, 则 $\int f \in \mathbf{R}_+$ 是当 $n \to +\infty$ 时的 $\int f_n$ 的极限, 其中 $(f_n)_{n\in\mathbf{N}}$ 是 $\mathrm{Esc}(D,[0,M])$ 中任意一个几乎处处收敛于 f 的序列.

(L2) 如果 $f \in \mathrm{Mes}(\mathbf{R}^m,\overline{\mathbf{R}}_+)$, 则 $\int f \in \overline{\mathbf{R}}_+$ 是当 $N \to +\infty$ 时的通项为 $\int_{D_N}\inf(f,N)$ 的递增序列的极限, 其中 D_N 是顶点为 $(\pm N,\dots,\pm N)$ 的砌块.

由此我们推导出满足定理 III.1.18 结论的映射 $f \mapsto \int f$ 的唯一性. 它因而导致了对于命题 III.4.1 的证明, 从而证明了由性质 (L1) 和 (L2) 定义的积分满足定理 III. 1.18 和定理 III.1.23. 证明分为许多步, 最为精彩的是命题 III.4.1 的证明.

---

[24] 本书选取的叙述将勒贝格积分做得很像是黎曼积分: 从阶梯函数出发, 过渡到极限去定义一个可测函数的积分, 最后定义可测集和一个集合的测度的概念. 勒贝格的原来方法则是反过来的. 出发点如下: 为了计算从区间到 $\mathbf{R}_+$ 的函数的图像下的曲面的面积, 可以或者竖直地分割 (这是黎曼所做的), 或者水平地分割 (这是勒贝格所做的) 它. 如勒贝格所说, 要计算一堆不同面值的钱币的量值时, 黎曼积分是逐次取出每枚钱币并相加得出总的值, 而勒贝格积分则是先对钱币分类然后再对每类算出有多少. 显然, 水平分割成的集合远比竖直分割的复杂, 这只需画出就容易证明. 勒贝格原来的方法便于推广到更一般的架构中成立的测度论 (在概率论中这是不可或缺的). 在本书后面这能让我们避免集合论中有点令人烦恼的某些东西. 它的不便之处是限制到在那些类似于 $\mathbf{R}^n$ 的空间上 (至少在局部上如此) 出现的.

1. 有界阶梯函数的控制收敛定理

这一小节将致力于证明命题 III.4.1 的如下加强形式.

在后文中, D 总表示 $\mathbf{R}^n$ 的一个铺砌, 而 $M \in \mathbf{R}_+$.

[322] **命题 III.4.2.** — 设 $h \in \mathrm{Mes}(D,[0,M])$, 而 $(h_n)_{n\in\mathbf{N}}$ 是 $\mathrm{Esc}(D,[0,M])$ 中的一个几乎处处趋向 h 的序列. 则 $\int h_n$ 有一个极限并记其为 $\int h$, 它只依赖 h 而不依赖 $(h_n)_{n\in\mathbf{N}}$ 的选取. 进一步还有 $|h-h_n| \in \mathrm{Mes}(D,[0,M])$ 和 $\int |h-h_n| \to 0$.

注记 III.4.3. — (i) 由于对于所有的 n 有 $\int h_n \geqslant 0$, 故 $\int h \geqslant 0$.

(ii) 如果 $h_n \to f$ a.e. 以及 $h'_n \to g$ a.e., 则 $h_n + h'_n \to f+g$ a.e. 由此得到 $\int f+g = \int f + \int g$, 其中 $f, g \in \mathrm{Mes}(D,[0,M])$. 特别地, 如果 $g \geqslant f$, 则 $\int g = \int f + \int g - f \geqslant \int f$.

引理 III.4.4. — 如果 A 具有有限的外测度, 则对于任意的 $\varepsilon > 0$, 存在一个包含 A 的开集 U, 使得 $\lambda^+(U) \leqslant \lambda^+(A) + \varepsilon$.

证明 如果 $D = \prod_{j=1}^m [a_j, b_j[$ 是一个砌块, 则任给 $\eta > 0$ 可以找到一个包含 D 的开铺砌 $P = \prod_{j=1}^m]a'_j, b_j[$ 使得 $\lambda^+(P) \leqslant \lambda(D) + \eta$. 于是令 $(D_n)_{n\in\mathbf{N}}$ 是一个初等砌块的序列, 它满足 $A \subset \cup_{n\in\mathbf{N}} D_n$ 以及 $\lambda^+(A) \leqslant \sum_{n\in\mathbf{N}} \lambda(D_n) + \frac{\varepsilon}{2}$. 根据前面的讨论, 存在包含 D_n 的开铺砌 P_n, 使得 $\lambda^+(P_n) \leqslant \lambda(D_n) + \frac{\varepsilon}{2^{n+3}}$, 则 $U = \cup_{n\in\mathbf{N}} P_n$ 便为引理所求. □

引理 III.4.5. — 如果 $(X_n)_{n\in\mathbf{N}}$ 是一个递降的铺砌的序列, 使得 $\cap_{n\in\mathbf{N}} X_n$ 为零测度集, 则 $\lim_{n\to+\infty} \lambda(X_n) = 0$.

证明 设 $\mathscr{L}$ 是形如 $x_i = r$ 的超平面对于 $1 \leqslant i \leqslant m$, $r \in \mathbf{Z}[\frac{1}{2}]$ 的并. 由于 $\{1,\dots,m\} \times \mathbf{Z}[\frac{1}{2}]$ 可数, 故 $\mathscr{L}$ 的测度为 0. 现若 $n \in \mathbf{N}$, 且 $\overline{X}_n$ 代表 X_n 的闭包, 于是有 $\overline{X}_n \subset X_n \cup \mathscr{L}$, 从而

$$\cap_{n\in\mathbf{N}} \overline{X}_n \subset \cap_{n\in\mathbf{N}} (X_n \cup \mathscr{L}) \subset (\cap_{n\in\mathbf{N}} X_n) \cup \mathscr{L};$$

由此得知 $\cap_{n\in\mathbf{N}} \overline{X}_n$ 的测度为 0.

设 $\varepsilon > 0$. 由于 $\cap_{n\in\mathbf{N}} \overline{X}_n$ 的测度为 0, 故存在包含 $\cap_{n\in\mathbf{N}} \overline{X}_n$ 的开集 U_ε 满足 $\lambda^+(U_\varepsilon) < \varepsilon$. 令 F_ε 为 U_ε 在 $\overline{X}_0$ 中的补集. 我们因而有 $F_\varepsilon \cap (\cap_{n\in\mathbf{N}} \overline{X}_n) = \emptyset$, 这表明存在 $n_0 \in \mathbf{N}$ 使得 $F_\varepsilon \cap (\cap_{n\leqslant n_0} \overline{X}_n) = \emptyset$: 因为 $\overline{X}_0$ 为紧集而 F_ε 和 $\overline{X}_n$ 为在 $\overline{X}_0$ 中的闭集. 由于 $(\overline{X}_n)_{n\in\mathbf{N}}$ 递降, 由此得到 $F_\varepsilon \cap \overline{X}_{n_0} = \emptyset$, 故 $X_n \subset \overline{X}_n \subset U_\varepsilon$, 其中 $n \geqslant n_0$ 任意. 因此我们证明了, 对于任意的 $\varepsilon > 0$ 存在 n_0, 使得对于 $n \geqslant n_0$ 有 $\lambda(X_n) \leqslant \lambda^+(U_\varepsilon) < \varepsilon$. 得到结论. □

引理 III.4.6. — 如果 $(h_n)_{n\in\mathbf{N}}$ 是 $\mathrm{Esc}(D,[0,M])$ 中的几乎处处趋向 0 的递降序列, 则 $\lim_{n\to+\infty} \int h_n = 0$.

证明 如果 $\varepsilon > 0$, 且 $n \in \mathbf{N}$, 令 $X_{n,\varepsilon} = \{x \in D, h_n(x) \geqslant \varepsilon\}$. 于是 $(X_{n,\varepsilon})_{n\in\mathbf{N}}$ 是一个递降的铺砌, 并且因为几乎处处 h_n 趋向 0, 故 $\cap_{n\in\mathbf{N}} X_{n,\varepsilon}$ 的测度为 0. 根据引理

III.4.5, 这表明 $\lim_{n\to+\infty}\lambda(X_{n,\varepsilon})=0$; 从而存在 $n\in\mathbf{N}$ 使得 $\lambda(X_{n+p,\varepsilon})\leqslant\varepsilon$, $p\in\mathbf{N}$. 由于当 $x\in X_{n+p,\varepsilon}$ 时 $h_{n+p}(x)\leqslant M$, 以及当 $x\notin X_{n+p,\varepsilon}$ 时 $h_{n+p}(x)\leqslant\varepsilon$, 故有 $\int h_{n+p}\leqslant\varepsilon(\lambda(D)+M)$, 其中 $p\in\mathbf{N}$ 任意. 证完. □

引理 III.4.7. — 如果 $(h_n)_{n\in\mathbf{N}}$ 是 $\mathrm{Esc}(D,[0,M])$ 中的一个几乎处处趋向 0 的序列, 使得 $\sum_{n\in\mathbf{N}}\int|h_{n+1}-h_n|<\infty$, 则 $\lim_{n\to+\infty}\int h_n=0$.

证明 设若相反, 则存在 $C>0$ 及无限多个 $n\in\mathbf{N}$ 使得 $\int h_n\geqslant C$. 必要时可抽出序列 h_n 的一个子序列, 故不妨设对于任意的 $n\in\mathbf{N}$ 都有 $\int h_n\geqslant C$ (这也没有改变条件 $\sum_{n\in\mathbf{N}}\int|h_{n+1}-h_n|<+\infty$: 因为如果 $\varphi:\mathbf{N}\to\mathbf{N}$ 严格递增, 则有 $|h_{\varphi(n+1)}-h_{\varphi(n)}|\leqslant\sum_{k=\varphi(n)}^{\varphi(n+1)-1}|h_{k+1}-h_k|$). 由于级数 $\sum_{n\in\mathbf{N}}\int|h_{n+1}-h_n|$ 收敛, 必要时以 $n+n_0$ 替代 n, 故不妨进一步假设 $\sum_{k\in\mathbf{N}}\int|h_{k+1}-h_k|\leqslant\frac{C}{2}$. 于是令 $g_n=\inf_{k\leqslant n}h_k$. 由构造知, g_n 是 $\mathrm{Esc}(D,[0,M])$ 的一个递降序列, 由于 $g_n\leqslant h_n$, 它几乎处处趋向 0. 根据引理 III.4.6, 这表明 $\lim_{n\to+\infty}\int g_n=0$. 另外, 我们有 [323] $g_n(x)\geqslant h_0(x)-\sum_{k=0}^{n-1}|h_{k+1}(x)-h_k(x)|$ (等号成立当且仅当序列 $(h_n(x))_{n\in\mathbf{N}}$ 递降). 由此得到 $\int g_n\geqslant\int h_0-\sum_{k=0}^{n-1}\int|h_{k+1}-h_k|\geqslant C-\frac{C}{2}$, 其中 $n\in\mathbf{N}$ 任意. 矛盾. 从而得证. □

命题 III.4.2 的证明 如果 $n\leqslant p$, 则令

$$f_{n,p}=\inf_{n\leqslant k\leqslant p}h_k \quad 和 \quad g_{n,p}=\sup_{n\leqslant k\leqslant p}h_k.$$

于是, 当 n 固定时, $f_{n,p}$ (分别地, $\int g_{n,p}$) 是 $\mathrm{Esc}(D,[0,m])$ 中的一个递降 (分别地, 递增) 的序列, 而当 p 固定时, $f_{n,p}$(分别地, $g_{n,p}$) 则是一个递增 (分别地, 递降) 的序列. 特别地, 当 n 固定时, 序列 $\int f_{n,p}$(分别地, $\int g_{n,p}$) 是 $[0,M\lambda(D)]$ 中的一个递降 (分别地, 递增) 序列; 它具有一个极限并且是一个柯西序列. 因此可以找到 $\varphi_0(n)\geqslant n$ 使得对于任意的 $p_1,p_2\geqslant\varphi_0(n)$ 有

$$\Big|\int f_{n,p_1}-\int f_{n,p_2}\Big|\leqslant 2^{-n} \quad 和 \quad \Big|\int g_{n,p_1}-\int g_{n,p_2}\Big|\leqslant 2^{-n}.$$

以 a_n 记递增序列 $\int g_{n,p}-f_{n,p}$ 当 p 趋向 $+\infty$ 时的极限, 并选取 $\varphi:\mathbf{N}\to\mathbf{N}$ 满足 $\varphi(n)\geqslant\varphi_0(n)$, 从而 $\int u_n\geqslant\frac{1}{2}a_n$, 其中 $u_n=g_{n,\varphi(n)}-f_{n,\varphi(n)}$. 由构造知, $u_n\in\mathrm{Esc}(D,[0,M])$, 并且由于 h_n 几乎处处有极限, 故几乎处处 $u_n\to 0$.

如果 $n\in\mathbf{N}$, 且 $p\geqslant\varphi(n)$, 则

$$\int|g_{n+1,\varphi(n+1)}-g_{n,\varphi(n)}|\leqslant\int|g_{n+1,\varphi(n+1)}-g_{n+1,p}|+\int|g_{n+1,p}-g_{n,p}|+\int|g_{n,p}-g_{n,\varphi(n)}|.$$

现在由假设条件有

$$\int|g_{n+1,\varphi(n+1)}-g_{n+1,p}|=\int|g_{n,p}-g_{n,\varphi(n)}|\leqslant 2^{-n-1}+2^{-n}\leqslant 2^{1-n},$$

并且由于序列 $(g_{n,p})_{n\leqslant p}$ 递降, 故 $|g_{n+1,p}-g_{n,p}|=g_{n,p}-g_{n+1,p}$. 由此得到, 对于任意的 $p\geqslant \max_{n\leqslant N}\varphi(n)$, 有控制函数

$$\sum_{n=0}^{N-1}\int|g_{n+1,\varphi(n+1)}-g_{n,\varphi(n)}|\leqslant\sum_{n=0}^{N-1}(2^{1-n}+\int g_{n,p}-g_{n+1,p})$$
$$\leqslant 4+\int g_{0,p}-g_{N,p}\leqslant 4+M\lambda(D),$$

其中的最后一个不等式来自 $g_{0,p}-g_{N,p}\in \mathrm{Esc}(D,[0,M])$. 同样可证明

$$\sum_{n=0}^{N-1}\int|f_{n+1,\varphi(n+1)}-f_{n,\varphi(n)}|\leqslant 4+M\lambda(D).$$

因此推出

$$\sum_{n=0}^{+\infty}\int|u_n-u_{n+1}|\leqslant\sum_{n=0}^{+\infty}(\int|f_{n+1,\varphi(n+1)}-f_{n,\varphi(n)}|+|g_{n+1,\varphi(n+1)}-g_{n,\varphi(n)}|)$$
$$\leqslant 8+2M\lambda(D)<+\infty,$$

这让我们可以利用引理 III.4.7 证明 $\int u_n\to 0$ 从而 $a_n\to 0$. 然而我们有

$$a_n=\sup_{p\geqslant n}((\int\sup_{n\leqslant k\leqslant p}h_k)-(\int\inf_{n\leqslant k\leqslant p}h_k))\geqslant(\sup_{k\geqslant n}\int h_k)-(\inf_{k\geqslant n}\int h_k).$$

因此得知序列 $(\int h_n)_{n\in\mathbf{N}}$ 的上极限和下极限相等, 从而 $(\int h_n)_{n\in\mathbf{N}}$ 有极限.

现在, 如果从 $\mathrm{Esc}(D,[0,M])$ 中几乎处处收敛于 h 的序列 $(h_n)_{n\in\mathbf{N}}$ 和 $(h'_n)_{n\in\mathbf{N}}$ [324] 出发, 则可构造出 $\mathrm{Esc}(D,[0,M])$ 中的第三个几乎处处收敛于 h 的序列 $(h''_n)_{n\in\mathbf{N}}$: 对于 $n\in\mathbf{N}$, 令 $h''_{2n}=h_n$ 而 $h''_{2n+1}=h'_n$. 当 $n\to+\infty$ 时 $\int h''_n$ 的极限的存在性表明 $\lim_{n\to+\infty}\int h_n$ 与 $\lim_{n\to+\infty}\int h'_n$ 相等, 因而证明了此极限值依赖 h 而与序列 $(h_n)_{n\in\mathbf{N}}$ 的选取无关.

将前面的结论应用于 $f_n=\inf_{k\geqslant n}h_k=\lim_{p\to+\infty}f_{n,p}$ 和 $g_n=\sup_{k\geqslant n}h_k=\lim_{p\to+\infty}g_{n,p}$, 其中的元由构造知均属于 $\mathrm{Mes}(D,[0,M])$. 因此有 $\int g_n-f_n=\lim_{p\to+\infty}\int g_{n,p}-f_{n,p}=a_n$ 而 $a_n\to 0$. 另外由于几乎处处 $f_n\leqslant h_n\leqslant g_n$ 和 $f_n\leqslant h\leqslant g_n$, 这表明几乎处处 $|h-h_n|\leqslant g_n-f_n$, 故有 $\int|h-h_n|\leqslant a_n$, 因而 $\int|h-h_n|\to 0$.

命题得证. □

2. 可测集的测度和外测度

这一小节要证明定理 III.1.23, 按此定理, 对于所有的可测集 A 有 $\lambda(A)=\lambda^+(A)$. 如果 A 可测且 $A_N=A\cap[-N,N]^m$, 则按定义 $\lambda(A)=\lim_{n\to+\infty}\lambda(A_N)$. 另外, 从

命题 III.1.3 的 (i) 和 (ii) 可得到 $\lambda^+(A) = \sup_{N\in\mathbf{N}} \lambda^+(A_N)$. 因此只要证明对所有的 $N \in \mathbf{N}$ 有 $\lambda(A_N) = \lambda^+(A_N)$ 就可以证明 $\lambda(A) = \lambda^+(A)$. 换而言之, 不妨设 A 有界.

在后面我们固定 $\mathbf{R}^m$ 中一个铺砌 D, 而所考虑的集合均含在 D 中. 称 $A \subset D$ 是可铺砌的是说存在一个互不相交的初等砌块的序列 $(D_n)_{n\in\mathbf{N}}$ 使得 $A = \coprod_{n\in\mathbf{N}} D_n$; 称 A 的一个这样的分解为它的初等砌块分解.

引理 III.4.8. — 如果 $(A_n)_{n\in\mathbf{N}}$ 是 D 的一个可铺砌子集的序列, 则 $A = \cup_{n\in\mathbf{N}} A_n$ 可铺砌.

证明 将每个 A_n 写成可数个初等砌块 $D_{n,i}$ 的不交并, 其中 $i \in I_n$. 如果 $x \in A$, 令 D_x 是 $D_{n,i}, n \in \mathbf{N}, i \in I_n$ 中包含 x 的最大初等砌块 (D_x 的存在性来自初等砌块表现得像是水银珠的性质). 如果 $J \subset \cup_{n\in\mathbf{N}}(\{n\} \times I_n)$ 为使得存在 $x \in A$ 满足 $D_x = D_{n,i}$ 的 (n, i) 的集合. 那么 A 便是那些 $D_{n,i}$, $(n, i) \in J$ 的不交并, 从而 A 可铺砌. □

引理 III.4.9. — (i) 如果 $A \subset D$ 可铺砌, 则 A 可测, 并且对于 A 的所有初等砌块分解 $A = \coprod_{n\in\mathbf{N}} D_n$ 有 $\lambda^+(A) = \lambda(A) = \sum_{n\in\mathbf{N}} \lambda(D_n)$.

(ii) 如果 $A \subset D$, 则 $\lambda^+(A) = \inf \lambda(B)$, 其中 B 遍历满足 $A \subset B \subset D$ 的可铺砌集的集合.

证明 如果 $n \in \mathbf{N}$, 令 $f_n = \sum_{i\leqslant n} \mathbf{1}_{D_i}$. 于是 $(f_n)_{n\in\mathbf{N}}$ 是 $\mathrm{Esc}(D, [0, 1])$ 中在每点都趋向 $\mathbf{1}_A$ 的序列, 因此根据命题 III.4.2, $\int f_n = \sum_{i\leqslant n} \lambda(D_i)$ 趋向 $\int \mathbf{1}_D = \lambda(D)$. 由此推出 A 可测且 $\lambda(A) = \sum_{n\in\mathbf{N}} \lambda(D_n)$. (ii) 由回到 $\lambda^+(A)$ 的定义得到. 而 (i) 中的等式 $\lambda^+(A) = \lambda(A)$ 是 (ii) 的直接推论. □

引理 III.4.10. — 如果 $f \in \mathrm{Mes}(D, \mathbf{R}_+)$, 且 $M \in \mathbf{R}_+$, 则 $\int f \geqslant M\lambda^+(\{x, f(x) > M\})$.

证明 $M = 0$ 的情形显然. 以 M^{-1} 乘 f 则可化为 $M = 1$ 的情形, 并在必要时将 f 换作 $\inf(f, 2)$, 故不妨设 f 在 $[0, 2]$ 中取值. 设 $(h_n)_{n\in\mathbf{N}}$ 是 $\mathrm{Esc}(D, [0, 2])$ 中几乎处处趋向 f 的一个序列. 根据命题 III.4.2, 于是有 $\int |f - h_n| \to 0$, 又若有必要抽出 h_n 的子序列, 故不妨设 $\int |f - h_n| \leqslant 2^{-2-n}$. 令 $A = \{x, f(x) > 1\}$, 如果 $n \in \mathbf{N}$, 令 $A_n = \{x, h_n(x) > 1\}$. 于是 A_n 是个铺砌, 并存在零测度集 $B \subset A$ 使得 $A - B \subset \cup_{n\geqslant N} A_n$, 其中 $N \in \mathbf{N}$ 任意. 因为 $\cup_{n\geqslant N} A_n$ 可铺砌 (引理 III.4.8), 故引理 III.4.9 的 (ii) 给了我们一个下界 $\lambda(\cup_{n\geqslant N} A_n) \geqslant \lambda^+(A - B) = \lambda^+(A)$, 其中 $N \in \mathbf{N}$ 任意, 并且因为 $\sup_{n\geqslant N} h_n \geqslant \mathbf{1}_{\cup_{n\geqslant N} A_n}$, 因而对于所有的 $N \in \mathbf{N}$ 我们也有 $\int \sup_{n\geqslant N} h_n \geqslant \lambda^+(A)$.

另外, 由命题 III.4.2 得知 $\int \sup_{n\geqslant N} h_n$ 是当 $k \to +\infty$ 时 $\int \sup_{k\geqslant n\geqslant N} h_n$ 的极限, [325] 而因为

$$\sup_{k\geqslant n\geqslant N} h_n \leqslant h_N + |h_{N+1} - h_N| + \cdots + |h_k - h_{k+1}|$$

和

$$\int |h_{n+1} - h_n| \leqslant \int |h_{n+1} - h| + \int |h - h_n| \leqslant 2^{-1-n},$$

故我们得到 $\int \sup_{n \geqslant N} h_n \leqslant 2^{-N} + \int h_N$, 从而对所有的 $N \in \mathbf{N}$ 有 $\lambda^+(A) \leqslant 2^{-N} + \int h_N$. 最后, 由于 $\int h_N \to \int f$, 那么过渡到极限便得到所要的不等式 $\lambda^+(A) \leqslant \int f$, 得到了结论. □

回到定理 III.1.23 的证明. 如果 B 是个包含 A 的可铺砌集, 由于 $\mathbf{1}_A \leqslant \mathbf{1}_B$, 故有 $\lambda(A) \leqslant \lambda(B)$. 对所有这些包含了 A 的可铺砌集 B 取下界, 根据引理 III.4.9 的 (ii) 便得到了 $\lambda(A) \leqslant \lambda^+(A)$.

不等式 $\lambda^+(A) \leqslant \lambda(A)$ 由应用引理 III.4.10 于 $f = (1+\varepsilon)\mathbf{1}_A$ 和 $M = 1$, 然后让 ε 趋向 0 得到.

证完. □

3. 对于具紧支集的有界函数的单调收敛定理

引理 III.4.11. — 如果 $(h_n)_{n\in\mathbf{N}}$ 是 $\mathrm{Mes}(\mathbf{R}^m, \mathbf{R}_+)$ 中的一个序列, 那么它几乎处处单趋向 h, 并且如果 $\int h_n \to 0$, 那么 $h = 0$ a.e..

证明 h 是序列 $(h_n)_{n\in\mathbf{N}}$ 的所有子序列的几乎处处存在的单极限, 若有必要抽出一个子序列, 故不妨设, 对于任意的 $n \in \mathbf{N}$ 有 $\int h_n \leqslant 2^{-n}$. 为了证明 $h = 0$ a.e., 只需证明对于任意的 $j \in \mathbf{N}$, 使得 $h(x) > 2^{-j}$ 的 x 的集合 X_j 是一个零测度集即可. 然而由引理 III.4.10 知 $\lambda^+(\{x, h_n(x) > 2^{-j}\}) \leqslant 2^j \int h_n \leqslant 2^{j-n}$. 因为 $\sum 2^{j-n} < +\infty$, 故根据博雷尔–坎泰利定理知, 使得对无限多个 $n \in \mathbf{N}$ 有 $h_n(x) > 2^{-j}$ 的 x 的集合测度为 0, 并且由于 X_j 包含在这个集合之中 (近乎是那些使 $h_n(x) \not\to h(x)$ 的 x 的集合, 这是一个零测度集), 于是得到结论. □

引理 III.4.12. — 如果 $(g_n)_{n\in\mathbf{N}}$ 是 $\mathrm{Esc}(\mathbf{R}^m)$ 中使得 $\sum_{n\in\mathbf{N}} \int |g_n| < +\infty$ 的序列, 则级数 $\sum_{n\in\mathbf{N}} g_n(x)$ 几乎处处绝对收敛.

证明 令 $C = \sum_{n\in\mathbf{N}} \int |g_n|$. 如果 $M \in \mathbf{R}_+$, 令 $X_{M,n}$ 为使得 $\sum_{k\leqslant n} |g_k(x)| \geqslant M$ 的 $x \in \mathbf{R}^m$ 的集合. 于是 $X_{M,n}$ 是一个递增的铺砌的序列, 并有

$$M\lambda(X_{M,n}) \leqslant \int_{X_{M,n}} \sum_{k\leqslant \mathbf{N}} |g_k| \leqslant \int \sum_{k\leqslant n} |g_k| = \sum_{k\leqslant n} \int |g_k| \leqslant C,$$

其中 $n \in \mathbf{N}$ 任意. 由此得到 $\lambda^+(\cup_{n\in\mathbf{N}} X_{M,n}) \leqslant M^{-1}C$, 并且由于使得 $\sum_{n\in\mathbf{N}} |g_n(x)| = +\infty$ 的 $x \in \mathbf{R}^m$ 的集合 A 是那些 $X_{M,n}$ 的交, 其中 $M \in \mathbf{R}_+$, 故对于任意的 $M \in \mathbf{R}_+$ 有 $\lambda^+(A) \leqslant M^{-1}C$. 这表明 A 的测度为 0, 得到结论. □

引理 III.4.13. — 如果 $(h_k)_{k\in\mathbf{N}}$ 是 $\mathrm{Mes}(D, [0, M])$ 中的递增序列, 则序列 $(h_k)_{k\in\mathbf{N}}$

的极限可测, 并且

$$\int h = \lim \int h_k = \sup \int h_k.$$

证明 序列 $\int h_k$ 递增且被 $M\lambda(D)$ 控制; 因而它具有一个有限的极限 ℓ, 并且必要时抽出一个子序列而不妨设对于任意的 $k \in \mathbf{N}$ 有 $\ell - \int h_n \leqslant 2^{-k}$.

现在由于假设了 h_k 可测, 故存在一个几乎处处趋向 h_k 的阶梯函数 $f_{k,\ell}$ 的序列. 由于 h_k 的支集在 D 中并取值于 $[0, M]$, 并且在必要时将 $f_{k,\ell}$ 换作如下函数: 当 $x \notin D$ 或者 $\mathrm{Re}(f_{k,\ell}(x)) \leqslant 0$ 时取值 0, 而当 $\mathrm{Re}(f_{k,\ell}(x)) \in [0, M]$ 且 $x \in D$ 时取值 $\mathrm{Re}(f_{k,\ell}(x))$, 但当 $\mathrm{Re}(f_{k,\ell}(x)) \geqslant M$ 且 $x \in D$ 时取值 M, 故不妨设 $f_{k,\ell} \in \mathrm{Esc}(D, [0, M])$. 根据命题 III.4.2, $\lim_{\ell\to+\infty} \int |h_k - f_{k,\ell}| = 0$; 因此存在 $\ell(k)$ 使得, 如果令 $f_k = f_{k,\ell(k)}$, 则有 $\int |f_k - h_k| \leqslant 2^{-k}$. 我们于是有 [326]

$$\int |f_{k+1} - f_k| \leqslant \int |f_{k+1} - h_{k+1}| + \int |h_{k+1} - h_k| + \int |h_k - f_k| \leqslant 3 \cdot 2^{-k},$$

并因为 $\sum_{k\in\mathbf{N}} 3 \cdot 2^{-k} < +\infty$, 则引理 III.4.12 证明了 f_k 几乎处处有单极限 $f(x)$. 故函数 f 作为阶梯函数的几乎处处的单极限是可测的, 并且根据命题 III.4.2 知 $\int f_k \to \int f$. 由于 $\int f_k$ 和 $\int h_k$ 具有相同的极限, 因此为了完成证明只需证明 $f = h$ a.e. 即可. 然而 $f - h$ 是 $f_k - h_k$ 几乎处处的极限, 且按构造有 $\int |f_k - h_k| \to 0$, 那么用引理 III.4.11 便得结论. □

4. 可测函数的几乎处处极限

这一小节的目的是证明命题 III.1.12, 按它所说, 可测函数的几乎处处的单极限仍可测. 由于 $f : \mathbf{R}^m \to \mathbf{C}$ 可测当且仅当函数 $\mathrm{Re}^+(f), \mathrm{Re}^+(-f), \mathrm{Re}^+(if)$ 和 $\mathrm{Re}^+(-if)$ 可测, 以及由于一个正函数可测当且仅当它是阶梯函数的几乎处处的单极限, 故我们可假定这里所考虑的所有函数都是正的.

引理 III.4.14. — 设 f 是 $\mathbf{R}^m$ 上的正函数, 而对 $j \in \mathbf{N}$ 令 D_j 是顶点为 $(\pm 2^j, \ldots, \pm 2^j)$ 的铺砌.

(i) 如果 $\mathbf{1}_{D_j} f$ 对于每个 $j \in \mathbf{N}$ 可测, 则 f 可测.

(ii) 如果 $\mathbf{1}_{D_j} \inf(f, N)$ 对于所有 $j, N \in \mathbf{N}$ 可测, 则 f 可测.

证明 (i) 设对于 $j \in \mathbf{N}$, $(f_{j,k})_{k\in\mathbf{N}}$ 是几乎处处趋向 $\mathbf{1}_{D_j} f$ 的阶梯函数的序列. 又设 g_k 为阶梯函数, 它在 D_k 外为 0 而在 $D_j - D_{j-1}$, $j \leqslant k$ 上等于 $f_{j,k}$. 于是当 $x \in D_j - D_{j-1}$ 且 $k \geqslant j$ 时我们有 $g_k(x) = f_{j,k}(x)$, 这证明了 g_k 几乎处处趋向 f. 由此推出了 (i). [327]

(ii) 为证明 (ii), 我们考虑到 (i), 则可设 f 的支集在 D_j 中, 从而 $\mathbf{1}_{D_j} \inf(f, N) = \inf(f, N)$. 令 $(f_{N,k})_{k\in\mathbf{N}}$, $N \in \mathbf{N}$ 是几乎处处趋向 $\inf(f, N)$ 的阶梯函数. 又令 g_k 为如下的阶梯函数: 当 $f_{1,k} < 1$ 时取值 $f_{1,k}$, 而当 $f_{1,k} = 1$ 且 $f_{2,k} < 2$ 时取值 $f_{2,k}$, 又

当 $f_{1,k}=1, f_{2,k}=2$ 且 $f_{3,k}<3$ 时取值 $f_{3,k},\ldots$, 当对于任意 $i\leqslant k$ 有 $f_{i,k}=i$ 时取值 k. 设 A_N 为使得 $f_{N,k}$ 不趋向 $\inf(f,N)$ 的那些点的集合, 并令 $A=\cup_{N\in\mathbf{N}}A_N$. 于是由于可数个零测度集的并仍是零测度集, 故 A 为零测度集, 并且, 如果 $x\notin A$, 则当 k 充分大且 $f(x)\in]i-1,i[$ 时有 $g_k(x)=f_{i,k}(x)$, 而当 k 充分大且 $f(x)=i$ 时 $g_k(x)\in\{f_{i,k}(x),f_{i-1,k}(x)\}$. 由此推出当 $x\notin A$ 时 $g_k(x)$ 趋向 $f(x)$. 证完. □

转到命题 III.1.12 的证明.

设 (ϕ_k) 为几乎处处具有极限 ϕ 的可测函数序列. 为证明 ϕ 可测, 根据引理 III.4.14, 只要证明 $\mathbf{1}_{D_j}(\sup(\phi,N))$ 对任意的 $j,N\in\mathbf{N}$ 可测即可. 由于 $\mathbf{1}_{D_j}(\sup(\phi,N))$ 是 $\mathbf{1}_{D_j}(\sup(\phi_k,N))$ 的几乎处处存在的极限, 故可假定 ϕ 和这些 ϕ_k 的支集在 D_j 中并取值于 $[0,N]$.

然而我们已经证明了 (引理 III.4.13) 一个 $\mathrm{Mes}(D_j,[0,N])$ 中的递增序列 h_n 的极限可测; 这个结论对于递降序列也成立, 这只需将 h_n 换作 $N-h_n$ 就可看出. 由于 $\phi_k\to\phi$ a.e., 故 ϕ 也是 ϕ_k 的下确界, 从而作为递增序列 $g_k=\inf_{\ell\geqslant k}\phi_\ell$ 的几乎处处存在的极限也是可测的, 这里的每个 g_k 由于是递降序列 $g_{k,n}=\inf_{k\leqslant\ell\leqslant n}\phi_\ell$ 的极限是可测的. 证完. □

5. 单调收敛定理及其推论

定理 III.4.15. — 如果 $(f_n)_{n\in\mathbf{N}}$ 是 $\mathbf{R}^m$ 上的正可测函数的递增序列, 则 $\lim_{n\to+\infty}\int f_n=\int\lim_{n\to+\infty}f_n$.

证明 以 f 记序列 f_n 的极限; 它是 $\mathrm{Mes}(\mathbf{R}^m,\overline{\mathbf{R}}_+)$ 中的元. 如果 $n,N\in\mathbf{N}$, 令 $a_{n,N}=\int_{D_N}\inf(f_n,N)$. 按定义有 $\int f_n=\lim_{N\to+\infty}a_{n,N}$, 由于此序列是递增的, 从而 $\int f_n=\sup_{N\in\mathbf{N}}a_{n,N}$. 另外, 由于几乎处处 $f_n\to f$, 这表明在 D_N 上几乎处处 $\inf(f_n,N)\to\inf(f,N)$, 又由于 $\inf(f_n,N)$ 递增, 故由引理 III.4.13 得知 $\int_{D_N}\inf(f,N)=\sup_{n\in\mathbf{N}}a_{n,N}$. 因此有

$$\int f=\sup_{N\in\mathbf{N}}\big(\sup_{n\in\mathbf{N}}a_{n,N}\big)=\sup_{(n,N)\in\mathbf{N}\times\mathbf{N}}a_{n,N}=\sup_{n\in\mathbf{N}}\big(\sup_{N\in\mathbf{N}}a_{n,N}\big)=\sup_{n\in\mathbf{N}}\int f_n,$$

并由于序列 $(\int f_n)_{n\in\mathbf{N}}$ 递增, 我们便有 $\sup_{n\in\mathbf{N}}\int f_n=\lim_{n\to+\infty}\int f_n$, 从而定理得证. □

那么, 现在我们可以证明所构造的积分满足定理 III.1.18 的性质 (i)—(v) 了, 从而完成了勒贝格积分的存在性证明.

- 我们刚刚才证明了性质 (v).
- (i) 包含在构造中.
- 如果 $f,g\in\mathrm{Mes}(\mathbf{R}^m,\overline{\mathbf{R}}_+)$, 则

$$\inf(f+g,N)\leqslant\inf(f,N)+\inf(g,N)\leqslant\inf(f+g,2N),$$

因而

$$\mathbf{1}_{D_N}\inf(f+g,N)\leqslant\mathbf{1}_{D_N}\inf(f,N)+\mathbf{1}_{D_N}\inf(g,N)\leqslant\mathbf{1}_{D_{2N}}\inf(f+g,2N).$$

将 N 趋向 $+\infty$ 并利用单调收敛定理, 我们由此得到了不等式 $\int(f+g)\leqslant\int f+\int g\leqslant\int(f+g)$, 从而证明了 $\int(f+g)=\int f+\int g$. 归纳地得到了 $\int nf=n\int f, n\in\mathbf{N}$, 然后对于 $a\in\mathbf{Q}_+$ 有 $\int af=a\int f$, 最后利用递增的 $a\mapsto\int af$ 得到当 $a\in\mathbf{R}_+$ 时的 $\int af=a\int f$. 因此证明了积分的线性性 (性质 (ii)).

- 我们已知, 如果单调收敛定理成立 (上面已经证明了的性质 (v)) 则性质 (iii) 是已在第 2 小节中证明的定理 III.1.23(参看推论 III.1.22) 的特殊情形.
- 我们已注意到 (参看注记 III.1.19 的 (ii)), (iv) 可由 (ii) 和 (iii) 推出.

证完.



IV. 傅里叶变换

[329]

将一个周期函数表示为一个傅里叶级数对于解某些偏微分方程是个非常有效的工具 (傅里叶变换和周期函数的这个表示由傅里叶在 1811 年的关于热传导方程的文章中引进). 傅里叶反演公式 (由柯西 (1815) 和泊松 (Poisson, 1816) 在关于拉普拉斯方程的文章中证明) 则可将 $\mathbf{R}^m$ 上一个合理的函数写成酉线性特征标[1] 的连续和, 可用于 $\mathbf{R}^m$ 上的同一类型的偏微分方程. 这个傅里叶的 "工具箱" 适用于所有的局部紧交换群: 它涉及将在这样的群上的一个函数分解为特征标的 "和"[2]. 我们在有限群的架构下已经遇到过它了 (5 小节 §I.2); 在那里, 傅里叶级数对应于群 $\mathbf{R}/\mathbf{Z}$; 我们将在 $\mathbf{R}_+^*$ 上再次遇到它 (那时的名字是梅林变换, 参看注记 VII.2.5), 也将在 $\mathbf{Q}_p$ 上和对于 $\mathbf{Q}$ 的阿代尔群上遇到它 (参看 2 小节 §G.2).

IV.1. 依赖参数的积分

许多函数可由更为简单的函数的积分定义[3], 而控制收敛定理常常让我们能够证明它们的连续性和可导性.

定理 IV.1.1. — (参数积分的连续性) 设 X 是一个度量空间, 而 $x_0 \in X$. 设 $f: X \times \mathbf{R}^m \to \mathbf{C}$ 满足

- 函数 $t \mapsto f(x,t)$ 对于任意的 $x \in X$ 可测;
- 对于几乎所有的 $t \in \mathbf{R}^m$, 函数 $x \mapsto f(x,t)$ 在 x_0 连续;

[330]

---

[1] $\mathbf{R}^m$ 上的一个线性特征标是一个函数 $\chi: \mathbf{R}^m \to \mathbf{C}^*$, 它满足 $\chi(x+y) = \chi(x)\chi(y)$, 其中 $x, y \in \mathbf{R}^m$ 任意; 一个这样的特征标如果对任意的 $x \in \mathbf{R}^m$ 满足 $|\chi(x)| = 1$, 则称为酉的.

[2] 在概率论中, 傅里叶变换被称作特征函数.

[3] 欧拉的 Γ 函数便是一例, 它由 $\Gamma(s) = \int_{\mathbf{R}_+} e^{-t} t^s \frac{dt}{t}$ 定义, 或者, 可和函数 f 定义的傅里叶变换 $\hat{f}$, $\hat{f}(x) = \int_{\mathbf{R}} e^{-2i\pi xt} f(t)dt$ 为另一例.

- 存在 $h \in \mathscr{L}^1(\mathbf{R}^m)$ 使得, 对任意的 $x \in X$ 几乎处处有 $|f(x,t)| \leqslant h(t)$.

于是, 如果 $x \in X$, 则积分 $\int_{\mathbf{R}^m} f(x,t)dt$ 有定义, 并且函数 $F : X \to \mathbf{C} : F(x) = \int_{\mathbf{R}^m} f(x,t)\mathrm{d}t$ 在 x_0 连续.

证明 由于假设了函数 $t \mapsto f(x,t)$ 对于任意的 $x \in X$ 为可测, 并且其模被 $\mathscr{L}^1(R^m)$ 的一个元所控制, 故它属于 $\mathscr{L}^1$. 因此函数 F 确有定义. 要证明 F 在 x_0 连续, 只要证明 (因为 X 是个度量空间) 对于所有收敛于 x_0 的序列 $(y_n)_{n\in\mathbf{N}}$, 序列 $(F(y_n))_{n\in\mathbf{N}}$ 趋向 $F(x_0)$ 即可, 就是说

$$\lim_{n\to+\infty}\int_{\mathbf{R}^m} f(y_n,t)dt = \int_{\mathbf{R}^m} f(x_0,t)dt.$$

令 $g_n(t) = f(y_n,t)$, 而 $g(t) = g(x_0,t)$. 于是有

- 几乎处处 $\lim_{n\to+\infty} g_n(t) = g(t)$: 因为 $x \mapsto f(x,t)$ 在 x_0 对几乎所有的 t 连续.
- 几乎处处 $|g_n(t)| \leqslant h(t)$, 且 h 可和 (并与 n 无关).

因此它满足控制收敛定理的条件, 从而 $\lim_{n\to+\infty}\int_{\mathbf{R}^m} g_n(t)dt = \int_{\mathbf{R}^m} g(t)dt$, 故得结论. □

定理 IV.1.2. — (在和号内的求导) 设 I 是 $\mathbf{R}$ 的一个区间而 $f : I \times \mathbf{R}^m \to \mathbf{C}$ 满足

- $t \mapsto f(x,t)$ 对于所有的 $x \in I$ 可和,
- 存在一个零测度集 $A \subset \mathbf{R}^m$ 和可和函数 $h : \mathbf{R}^m \to \mathbf{R}_+$ 使得 $\frac{\partial f}{\partial x}(x,t)$ 在 $\mathbf{R}^m - A$ 中的每个点都存在, 且对所有的 $x \in I$[(4)] 和 $t \notin A$ 有 $|\frac{\partial f}{\partial x}(x,t)| \leqslant h(t)$.

于是在 I 上由 $F(x) = \int_{\mathbf{R}^m} f(x,t)dt$ 定义的函数 F 可导, 并且对于任意的 $x \in I$ 有

$$F'(x) = \int_{\mathbf{R}^m} \frac{\partial f}{\partial x}(x,t)dt.$$

证明 如有必要将 f 换作下面的函数: 当 $t \notin A$ 时取值为 $f(x,t)$, 而当 $t \in A$ 时取值为 0, 这没有改变这个积分的值, 故可设 $A = \emptyset$.

固定 $x \in I$. 令 $(x_n)_{n\in\mathbf{N}}$ 是 $I - \{x\}$ 中的序列, 且当 n 趋向 $+\infty$ 时趋向 x. 令 $g(t) = \frac{\partial f}{\partial x}(x,t)$, 而对 $n \in \mathbf{N}$ 令 $g_n(t) = \frac{f(x_n,t)-f(x,t)}{x_n - x}$. 于是 g_n 单趋向 g, 从而根据有限增量定理, 对于任意的 t 有

$$|g_n(t)| \leqslant \sup_{0\leqslant\theta\leqslant 1} |\frac{\partial f}{\partial x}(x+\theta(x_n - x),t)| \leqslant h(t).$$

[331] 因此我们处于可应用控制定理的条件中, 故 $\lim_{n\to+\infty}\int_{\mathbf{R}^m} g_n = \int_{\mathbf{R}^m} g$. 换句话说, 对于任意的那些在 $I - \{x\}$ 中的序列 $(x_n)_{n\in\mathbf{N}}$, 它们在 n 趋向 $+\infty$ 时趋向 x, 我们有

$$\lim_{n\to+\infty}\frac{F(x_n) - f(x)}{x_n - x} = \int_{\mathbf{R}^m} \frac{\partial f}{\partial x}(x,t)dt.$$

---

(4) 可求导是个局部性质, 要证明在一个区间 I 上的可导性只需在一系列取和为 I 的区间上证明即可. 换而言之, 不需要在整个 I 上的一个控制函数, 只要在其并为 I 的一系列区间上的即可. 这个脚注也可用于推论 IV.1.3, 对此我们可以从缩小 Ω 着手.

从而得到结果. □

如果 $\boldsymbol{\ell}=(\ell_1,\dots,\ell_n)\in\mathbf{N}^n$, 令 $|\boldsymbol{\ell}|=\ell_1+\cdots+\ell_n$, 而 $\partial^{\boldsymbol{\ell}}=(\frac{\partial}{\partial x_1})^{\ell_1}\dots(\frac{\partial}{\partial x_n})^{\ell_n}$.

推论 IV.1.3. — 设 Ω 是 $\mathbf{R}^n$ 中的一个开集, $k\in\mathbf{N}$, $f:\Omega\times\mathbf{R}^m\to\mathbf{C}$ 满足

- 对任意的 $x\in\Omega$, $t\mapsto f(x,t)$ 可和;
- 存在一个零测度集 $A\subset\mathbf{R}^m$ 以及一个可和的 $h:\mathbf{R}^m\to\mathbf{R}_+$ 使得当 $t\in\mathbf{R}^m-A$ 时函数 $x\mapsto f(x,t)$ 属于 Ω 上的 $\mathscr{C}^k$ 类, 并且对于任意的 $x\in\Omega$, $\boldsymbol{\ell}\in\mathbf{N}^n$, $|\boldsymbol{\ell}|\leqslant k$, $t\notin A$ 有 $\partial^{\boldsymbol{\ell}}f(x,t)|\leqslant h(t)$.

于是在 Ω 上定义的函数 $F:F(x)=\int_{\mathbf{R}^m}f(x,t)dt$ 对于任意的 $\boldsymbol{\ell}\in\mathbf{N}^n$, $|\boldsymbol{\ell}|\leqslant k$ 以及 $x\in\Omega$ 有

$$\partial^{\boldsymbol{\ell}}F(x)=\int_{\mathbf{R}^m}\partial^{\boldsymbol{\ell}}f(x,t)dt.$$

证明 立即由和号内求导定理归纳得到. □

习题 IV.1.4. — 设 $I=]0,1[$, 而定义 $f:I\times\mathbf{R}\to\mathbf{R}$ 为, 当 $t\leqslant 0$ 或 $t\geqslant x$ 时 $f(x,t)=0$, 而当 $0<t<x$ 时 $f(x,t)=1$. 显式计算 $F(x)=\int_{\mathbf{R}}f(x,t)dt$ 和 $F'(x)$. 能由此得出 $1=0$ 吗?

习题 IV.1.5. — (欧拉的 Γ 函数)

(i) 证明积分 $\Gamma(s)=\int_0^{+\infty}e^{-t}t^s\frac{dt}{t}$ 在 $s\in\mathbf{R}_+^*$ 确有定义.

(ii) 证明 Γ 在 $\mathbf{R}_+^*$ 上属于 $\mathscr{C}^\infty$ 类并在 $s=0$ 趋向 $+\infty$.

(iii) 证明当 $s>0$ 时有 $\Gamma(s+1)=s\Gamma(s)$; 由此得到, 当 $n\in\mathbf{N}$ 时 $\Gamma(n+1)=n!$.

(iv) 斯特林公式 (1730): 证明在 $+\infty$ 的邻域中 $\Gamma(s+1)\sim(\frac{s}{e})^s\sqrt{2\pi s}$. 做变量变换 $t=s+u\sqrt{s}$ (拉普拉斯方法), 并证明

$$-u\sqrt{s}+s\log(1+\frac{u}{\sqrt{s}})\leqslant\begin{cases}-\frac{u^2}{2}, & \text{当 } -\sqrt{s}<u\leqslant 0 \text{ 时},\\ -u+\log(1+u), & \text{当 } u\geqslant 0 \text{ 且 } s\geqslant 1 \text{ 时}.\end{cases}$$

(v) 由此推出高斯公式: $\frac{1}{\Gamma(s)}=\lim_{n\to+\infty}\frac{s(s+1)\dots(s+n)}{n!n^s}$, $s\in\mathbf{R}_+^*$.

习题 IV.1.6. — 令 $B(s,t)=\int_0^1x^{s-1}(1-x)^{t-1}dx$. 证明 $B(s,t)=\frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}$, 其中 $s>0$ 且 $t>0$. (将 $\Gamma(s+t)B(s,t)$ 写为一个二重积分.)

习题 IV.1.7. — 设 $f\in\mathscr{L}^1(\mathbf{R}^m)$ 而 $g\in\mathscr{C}_c^k(\mathbf{R}^m)$, 其中 $k\in\mathbf{N}\cup\{\infty\}$. 证明卷积 $x\mapsto f*g(x)=\int f(x-y)g(y)dy$ 属于 $\mathbf{R}^m$ 上的 $\mathscr{C}^k$ 类.

习题 IV.1.8. — (i) 证明积分 $\int_0^{+\infty}\frac{\sin t}{t}dt$ 为半收敛的 (即 $\frac{\sin t}{t}$ 对每个 T 在 $[0,T]$ 上可和, 而当 $T\to+\infty$ 时 $\int_0^T\frac{\sin t}{t}dt$ 有极限).

(ii) 如果 $\lambda\geqslant 0$, 令 $F(\lambda)=\int_0^{+\infty}e^{-\lambda t}\frac{\sin t}{t}dt$. 证明 F 在 $\mathbf{R}_+^*$ 上属于 $\mathscr{C}^1$, 并计算 $F'(\lambda)$.

(iii) 证明 F 在 $+\infty$ 趋向 0; 由此算出 $F(\lambda)$, $\lambda>0$.

[332] (iv) 证明 F 在 0 连续; 由此算出 $\int_0^{+\infty} \frac{\sin t}{t} dt$.

习题 IV.1.9. — (贝塞尔函数) 设 $\nu \in \mathbf{C}$.

(i) 证明 $y \mapsto K_\nu(y) = \frac{1}{2}\int_0^{+\infty} e^{-y(t+t^{-1})/2} t^\nu \frac{dt}{t}$ 在 $\mathbf{R}_+^*$ 上属于 $\mathscr{C}^\infty$ 类.

(ii) 证明在 $y = +\infty$ 的邻域中 $K_\nu(y) \sim \sqrt{\frac{2\pi}{y}} e^{-y}$. (可以将此积分从 1 分开从而引向在 $[1, +\infty[$ 上的一个积分, 并做变量变换 $t = 1 + \frac{y}{\sqrt{x}}$.)

IV.2. 在 L^1 中的傅里叶变换

1. $\mathbf{R}$ 和 $\mathbf{R}^m$ 的线性特征标

如果 $x = (x_1, \ldots, x_m)$ 和 $t = (t_1, \ldots, t_m)$ 是 $\mathbf{R}^m$ 中的两个元, 以 $x \cdot t$ 表示它们的标量积 $\sum_{i=1}^m x_i t_i$; 我们有 $x \cdot t = t \cdot x$. 回想一下, 如果 $A \in \mathbf{M}_m(R)$, ${}^{\mathrm{t}}A$ 代表了 A 的转置矩阵, 因此有 ${}^{\mathrm{t}}Ax \cdot t = x \cdot At$, 其中 $x, t \in \mathbf{R}^m$.

命题 IV.2.1. — (i) $\mathbf{R}$ 的连续线性特征标是 $t \mapsto e^{\lambda t}$, 其中 $\lambda \in \mathbf{C}$, 而连续的酉线性特征标是 $t \mapsto e^{2i\pi x t}$, 其中 $x \in \mathbf{R}$.

(ii) $\mathbf{R}^m$ 的连续酉线性特征标是 $t \mapsto e^{2i\pi x \cdot t}$, 其中 $x \in \mathbf{R}^m$.

证明 设 $\chi : \mathbf{R} \to \mathbf{C}^*$ 是一个连续的线性特征标. 由此特别有 $\chi(0) = 1$, 而连续性表明存在 $j \in \mathbf{N}$ 使得当 $|t| \leqslant 2^{-j}$ 时, $|\chi(t) - 1| \leqslant \frac{1}{2}$. 以 $\log : \mathbf{C}^* \to \{x + iy, -\pi < y \leqslant \pi\}$ 表示复对数. 由于 $B(1, \frac{1}{2})$ 包含在扇形角 $|\arg(z)| \leqslant \frac{\pi}{4}$ 中, 故映射 $g = \log \circ \chi : B(1, \frac{1}{2}) \to \mathbf{C}$ 取值在带状 $\{x + iy, |y| \leqslant \frac{\pi}{4}\}$ 中. 现在, 对于任意的 $z_1, z_2 \in \mathbf{C}^*$, $\log(z_1 z_2) - \log z_1 - \log z_2 \in 2i\pi$, 并由于 $\chi(t_1 + t_2) = \chi(t_1)\chi(t_2)$, 故当 $t_1, t_2, t_1 + t_2 \in B(1, \frac{1}{2})$ 时有 $g(t_1 + t_2) = g(t_1) + g(t_2)$. 因此对 n 归纳得到 $g(2^{-j-n}) = 2^{-n} g(2^{-j})$ 对所有的 $n \in \mathbf{N}$ 成立, 而对于 k 归纳, 得到 $g(k 2^{-j-n}) = k g(2^{-j-n})$, 其中 $k \in \{-2^n, \ldots, 2^n\}$. 因此当 r 是 $[-1, 1]$ 中的一个二进制数时我们便有 $g(r 2^{-j}) = r g(2^{-j})$, 又由于 g 连续, 从而推出 $g(t) = \lambda t$, 其中 $\lambda = 2^j g(2^{-j})$, 而 $t \in [-2^{-j}, 2^{-j}]$ 任意. 由 g 的定义, 这表明 $\chi(t) = e^{\lambda t}$, 其中 $t \in [-2^{-j}, 2^{-j}]$ 任意. 最后, 如果 $t \in \mathbf{R}$, 则存在 $n \in \mathbf{N}$ 使得 $t/n \in [-2^{-j}, 2^{-j}]$, 并由于 $\chi(t) = \chi(t/n)^n$, 故 $\chi(t) = e^{\lambda t}$, 其中 $t \in \mathbf{R}$.

现在, 如果 χ 为酉的, 则对所有的 $t \in \mathbf{R}$ 应该有 $\lambda t \in i\mathbf{R}$, 从而存在 $x \in \mathbf{R}$ 使得 $\lambda = 2i\pi x$. 这便得到了 (i).

如果 $\chi : \mathbf{R}^m \to \mathbf{C}^*$ 是个连续的酉线性特征标, 则它在 $\mathbf{R}e_j$ 的限制定义了 $\mathbf{R}$ 上的一个连续的酉线性特征标, 其中 $j \in \{1, \ldots, m\}$. 故存在 $x_j \in \mathbf{R}$ 使得 $\chi(t_j e_j) = e^{2i\pi x_j t_j}$. 但 $t = \sum_{j=1}^m t_j e_j$, 因此 $\chi(t) = \prod_{j=1}^m \chi(t_j e_j) = e^{2i\pi x \cdot t}$, 其中 $x = (x_1, \ldots, x_m)$. 证完. □

2. 定义和主要性质

如果 $f \in \mathscr{L}^1(\mathbf{R}^m)$, 则对任意的 $x, t \in \mathbf{R}^m$ 有 $|e^{-2i\pi x\cdot t}f(t)| = |f(t)|$; 故积分 $\int_{\mathbf{R}^m} e^{-2i\pi x\cdot t}f(t)dt$ 对所有的 $x \in \mathbf{R}^m$ 确有定义.

f 的傅里叶变换是指函数 $\hat{f}$, 它对 $x \in \mathbf{R}^m$ 定义为 [333]

$$\hat{f}(x) = \int_{\mathbf{R}^m} e^{-2i\pi x\cdot t}f(t)dt.$$

它只依赖 f 在 $L^1(\mathbf{R}^m)$ 的类, 从而让我们可以用同一个公式去定义 $L^1(\mathbf{R}^m)$ 中一个元的傅里叶变换. 由于书写的原因我们常常以 $\mathscr{F}f$ 代替 f 的傅里叶变换 $\hat{f}$, 并定义 $\overline{\mathscr{F}}f$ 为 $\overline{\mathscr{F}}f(x) = \hat{f}(-x)$.

例题 IV.2.2. — $\mathbf{1}_{[\frac{-1}{2},\frac{1}{2}[}$ 的傅里叶变换是 $\alpha(x) = \frac{\sin \pi x}{\pi x}$, 这由直接计算可得.

设 $f \in L^1(\mathbf{R}^m)$. 变量变换可立即证明:

- $\mathscr{F}(f(at))(x) = |a|^{-m}\hat{f}(a^{-1}x)$, 其中 $a \in \mathbf{R}^*$: 傅里叶变换将一个伸缩变换为对于原伸缩的逆的伸缩;
- $\mathscr{F}(f(t+b))(x) = e^{2i\pi b\cdot x}\hat{f}(x)$ 和 $\mathscr{F}(e^{2i\pi c\cdot t}f(t))(x) = \hat{f}(x-c)$, 其中 $b, c \in \mathbf{R}^m$: 傅里叶变换将平移和乘以一个特征标的运算互换.

习题 IV.2.3. — 证明更一般地有: 如果 $f \in L^1(\mathbf{R}^m)$, 且 $A \in \mathbf{GL}_m(\mathbf{R})$, $b, c \in \mathbf{R}^m$ 以及 $g(t) = e^{2i\pi c\cdot t}f(At+b)$, 则 $\hat{g}(x) = |\det A|^{-1}e^{2i\pi\, {}^{\mathrm{t}}A^{-1}(x-c)\cdot b}\hat{f}({}^{\mathrm{t}}A^{-1}(x-c))$.

习题 IV.2.4. — 设 f 是 $\mathbf{R}$ 上一个有界的可和连续函数, 且 $x_0 \in \mathbf{R}$. 证明当 λ 趋向 0^+ 时函数

$$F(\lambda) = \int_{-\infty}^{+\infty} e^{2i\pi x_0 y - \lambda|y|}\hat{f}(y)dy$$

趋向一个极限 (将来会计算它). 由此推出, 当 $\hat{f}$ 恒等于 0 时, 则 f 也恒等于 0.

习题 IV.2.5. — 设 $f \in L^1(\mathbf{R})$. 证明 $\lim_{T\to+\infty} T^{-1}\int_{-T}^{T}|\hat{f}(x)|^2dx = 0$.

3. 黎曼 – 勒贝格定理

像以前那样, $\mathscr{C}_0(\mathbf{R}^m)$ 代表了在 $\mathbf{R}^m$ 上在无限远处趋向 0 的连续函数的空间.

命题 IV.2.6. — (i) 如果 $r \in \mathbf{N}$, 而 $\boldsymbol{k} \in \mathbf{Z}^m$, 则

$$\hat{e}_{r,\boldsymbol{k}}(x) = 2^{-rm}\prod_{j=1}^{m}(e^{-2^{1-r}i\pi(k_j+\frac{1}{2})x_j}\alpha(2^{-r}x_j)).$$

(ii) 如果 f 是一个阶梯函数, 则 $\hat{f} \in \mathscr{C}_0(\mathbf{R}^m)$.

证明 (i) 是例题 IV.2.2 中的公式

$$e_{r,\boldsymbol{k}}(t)=\prod_{j=1}\mathbf{1}_{[\frac{-1}{2},\frac{1}{2}[}(2^r t_j-k_j-\frac{1}{2})$$

[334] 和伸缩 — 平移公式的推论. (ii) 则是由 (i), 以及这些 $e_{r,\boldsymbol{k}}$ 构成了 $\mathrm{Esc}(\mathbf{R}^m)$ 的一个生成元族, 并且 α 是 $\mathbf{R}$ 上一个在无限远趋向 0 的连续函数得到的结果. □

定理 IV.2.7. — (黎曼 - 勒贝格) 映射 $f\mapsto\hat{f}$ 是从 $L^1(\mathbf{R}^m)$ 到 $\mathscr{C}_0(\mathbf{R}^m)$ 的一个满足 1-利普希茨条件的线性映射. 换而言之, 如果 $f\in L^1(\mathbf{R}^m)$, 则 $\hat{f}$ 是 $\mathbf{R}^m$ 上的一个连续函数, 它在无限远趋向 0, 并有 $\|\hat{f}\|_\infty\leqslant\|f\|_1$.

证明 $f\mapsto\hat{f}$ 的线性性来自积分的线性性, 而不等式 $\|\hat{f}\|_\infty\leqslant\|f\|_1$ 来自控制关系

$$\Big|\int_{\mathbf{R}^m}e^{-2i\pi x\cdot t}f(t)dt\Big|\leqslant\int_{\mathbf{R}^m}|e^{-2i\pi x\cdot t}f(t)|dt=\int_{\mathbf{R}^m}|f(t)|dt=\|f\|_1.$$

现在, 如果 f 是一个阶梯函数则命题 IV.2.6 表明了 $\hat{f}\in\mathscr{C}_0(\mathbf{R}^m)$. 由于阶梯函数在 $L^1(\mathbf{R}^m)$ 中稠密, 又由于 $f\mapsto\hat{f}$ 是从 $L^1(\mathbf{R}^m)$ 到 $\mathbf{R}^m$ 上的有界函数空间 $\mathscr{B}(\mathbf{R}^m)$(赋予了范数 $\|\ \|_\infty$) 的连续线性映射, 而且在空间 $\mathscr{B}(\mathbf{R}^m)$ 中 $\mathscr{C}_0(\mathbf{R}^m)$ 为闭集, 故由此得到对于任意的 $f\in L^1(\mathbf{R}^m)$, $\hat{f}\in\mathscr{C}_0(\mathbf{R}^m)$(我们可以把这个推理做得不太抽象: 考虑一个阶梯函数的序列 f_n, 它在 $L^1(\mathbf{R}^m)$ 中收敛于 f; 于是 $\hat{f}_n\to\hat{f}$ 是一致的, 从而利用在无限远趋向 0 的连续函数的一致极限仍是在无限远趋向 0 的连续函数这个事实 (参看小词典的习题 16.4) 便可得结论). 证完. □

4. 傅里叶变换和求导

傅里叶变换的基本性质之一是正则性与到无限远的递降性之间的交替变化 (即函数越正则, 它的傅里叶变换到无限远就越小, 反之, 一个函数到无限远越小则它的傅里叶变换就越正则), 而求导与乘以多项式的运算也以同样方式交替, 如果结合傅里叶反演公式 (命题 IV.3.25), 它则极易于用作研究某些偏微分方程[5]. 我们特别有如下的结果.

定理 IV.2.8. — (i) 如果 $f\in\mathscr{C}^k(\mathbf{R}^m)$ 具有对每个 $\leqslant k$ 阶的可和偏导数, 则 $(1+\|x\|^2)^{k/2}\hat{f}(x)$ 在无限远趋向 0, 并且 $\mathscr{F}(\partial^{\boldsymbol{\ell}}f)=(2i\pi x)^{\boldsymbol{\ell}}\hat{f}$, 其中 $\boldsymbol{\ell}\in\mathbf{N}^m$ 满足

[335] $|\boldsymbol{\ell}|\leqslant k$[6].

---

[5] 设 $P=\sum_{\boldsymbol{\ell}}a_{\boldsymbol{\ell}}X^{\boldsymbol{\ell}}\in\mathbf{C}[X_1,\ldots,X_m]$, 且令 $P(\partial)$ 表示 $\sum_{\boldsymbol{\ell}}a_{\boldsymbol{\ell}}\partial^{\boldsymbol{\ell}}$. 如果我们要求偏微分方程 $P(\partial)u=\phi$ 的解, 其中 ϕ 已知, 并假定其足够好, 则我们可以形式地在两端应用傅里叶变换, 从而得到 $P(2i\pi x)\hat{u}(x)=\hat{\phi}(x)$. 再应用傅里叶反演公式, 便给出了 $u=\overline{\mathscr{F}}(\frac{\hat{\phi}(x)}{P(2i\pi x)})$. 上面是一个纯粹的形式的书写游戏, 但却给出了在物理问题中的许多有用的结果. 解偏微分方程的这个方法在广义函数理论的架构下取得了极大的成功.

[6] 回忆, $(2i\pi x)^{\boldsymbol{\ell}}=\prod_{j=1}^m(2i\pi x_j)^{\ell_j}$, 其中 $x=(x_1,\ldots,x_m)$, $\boldsymbol{\ell}=(\ell_1,\ldots,\ell_m)$.

(ii) 如果 $(1+\|t\|^2)^{k/2}f(t)$ 可和, 则 $\hat{f}$ 属于 $\mathscr{C}^k$ 类, 并且 $\partial^{\boldsymbol{\ell}}\hat{f}(x)=(-2i\pi)^{|\boldsymbol{\ell}|}\mathscr{F}(t^{\boldsymbol{\ell}}f)$, 其中 $|\boldsymbol{\ell}|\leqslant k$.

证明　如果 $f\in\mathscr{C}_c^k(\mathbf{R}^m)$, 则由分部积分法便得到 $\mathscr{F}(\partial^{\boldsymbol{\ell}}f)=(2i\pi x)^{\boldsymbol{\ell}}\hat{f}$ (对 $\partial^{\boldsymbol{\ell}}f$ 积分并对 $e^{-2i\pi x\cdot x}$ 求导). 例如, 如果 $f\in\mathscr{C}_c^1(\mathbf{R}^2)$, 那么由富比尼定理得到

$$\begin{aligned}\widehat{\partial_1 f}(x_1,x_2)&=\int_{\mathbf{R}^2}e^{-2i\pi(x_1t_1+x_2t_2)}\frac{\partial f}{\partial t_1}(t_1,t_2)dt_1dt_2\\&=\int_{\mathbf{R}}e^{-2i\pi x_2x_2}(\int_{\mathbf{R}}e^{-2i\pi x_1t_1}\frac{\partial f}{\partial t_1}(t_1,t_2)dt_1)dt_2.\end{aligned}$$

对括号里的积分进行分部积分便给出了

$$\int_{\mathbf{R}}e^{-2i\pi x_1t_1}\frac{\partial f}{\partial t_1}(t_1,t_2)dt_1=[e^{-2i\pi x_1t_1}f(t_1,t_2)]_{t_1=-\infty}^{+\infty}+2i\pi x_1\int_{\mathbf{R}}e^{-2i\pi x_1t_1}f(t_1,t_2)dt_1,$$

并由于 f 的支集为紧集, 右端的第一项为 0. 重新代入到二重积分的第二项中, 并再用富比尼定理得到

$$\begin{aligned}\widehat{\partial_1 f}(x_1,x_2)&=\int_{\mathbf{R}}e^{-2i\pi x_2t_2}(2i\pi x_1\int_{\mathbf{R}}e^{-2i\pi x_1t_1}f(t_1,t_2)dt_1)dt_2\\&=2i\pi x_1\int_{\mathbf{R}^2}e^{-2i\pi(x_1t_1+x_2t_2)}f(t_1,t_2)dt_1dt_2=2i\pi x_1\hat{f}(x_1,x_2).\end{aligned}$$

一般情形可以以同样的方式归纳处理.

为了处理一般情形的 f, 我们选取在 $[-1,1]^m$ 上取值为 1 的函数 $\phi\in\mathscr{C}_c^k(\mathbf{R}^m)$, 并定义 f_j 为 $f_j(x)=f(x)\phi(2^{-j}x)$, 其中 $j\in\mathbf{N}$. 于是 $f_j\in\mathscr{C}_c^k(\mathbf{R}^m)$, 再利用莱布尼茨公式对于乘积求导数. 稍加计算便证明了 $\partial^{\boldsymbol{\ell}}f_j$ 单趋向 $\partial^{\boldsymbol{\ell}}f$, 以及 $\partial^{\boldsymbol{\ell}}$ 被 f 的 $\boldsymbol{k}$, $|\boldsymbol{k}|\leqslant|\boldsymbol{\ell}|$ 阶导数的和所控制, 这表明 $\partial^{\boldsymbol{\ell}}f_j$ 在 $L^1(\mathbf{R}^m)$ 中趋向 $\partial^{\boldsymbol{\ell}}f$. 取极限, 于是 (利用 $\phi\mapsto\hat{\phi}$ 的连续性, 而它则来自从 $L^1(\mathbf{R}^m)$ 到 $\mathscr{C}_0(\mathbf{R}^m)$ 的映射 $\phi\mapsto\hat{\phi}$ 的连续性) 推出了恒等式 $\mathscr{F}(\partial^{\boldsymbol{\ell}}f)=(2i\pi x)^{\boldsymbol{\ell}}\hat{f}$. 因为对任意的 $\boldsymbol{\ell}\in\mathbf{N}^m$, $|\boldsymbol{\ell}|\leqslant k$, $\mathscr{F}(\partial^{\boldsymbol{\ell}}f)$ 在无限远处趋向 0, 故 $|x|^{\boldsymbol{\ell}}\hat{f}$ 也同样如此, 又因为 $(1+\|x\|^2)^{k/2}\leqslant(1+\sum_{j=1}^m|x_j|)^k$, 从而 $|(1+\|x\|^2)^{k/2}\hat{f}(x)|$ 也在无限远处趋向 0.

至于 (ii), 一旦注意到 $\partial^{\boldsymbol{\ell}}(e^{-2i\pi x\cdot t})=(-2i\pi t)^{\boldsymbol{\ell}}e^{-2i\pi x\cdot t}$, 它就是一个对于和号内求导数定理的简单应用. □

IV.3. 反演公式

1. 傅里叶级数

称 $f:\mathbf{R}\to\mathbf{C}$ 为周期为 1 的周期函数是说, 对所有的 $x\in\mathbf{R}$ 有 $f(x+1)=f(x)$. 于是对所有的 $x\in\mathbf{R}$, $n\in\mathbf{N}$ 有 $f(x+n)=f(x)$, 从而 f 是周期为 $\mathbf{Z}$ 的周期函数.

[336] 我们也可以将一个周期为 1 的周期函数看作是从 $\mathbf{T}=\mathbf{R}/\mathbf{Z}$ 到 $\mathbf{C}$ 的函数 (这常常是令人十分舒服的做法). 从前一个观点过渡到另一个的过程如下: 记 $\pi:\mathbf{R}\to\mathbf{T}$ 为将 x 映成它的 mod $\mathbf{Z}$ 的类; 如果 f 是 $\mathbf{T}$ 上的一个函数, 那么 $f\circ\pi:\mathbf{R}\to\mathbf{C}$ 便是一个周期为 1 的周期函数, 反之, 如果 $g:\mathbf{R}\to\mathbf{C}$ 是周期为 1 的周期函数, 则存在唯一的 $f:\mathbf{T}\to\mathbf{C}$, 使得 $g=f\circ\pi$.

赋予 $\mathbf{T}$ 以商拓扑, 这表明 $f:\mathbf{T}\to\mathbf{C}$ 连续当且仅当 $f\circ\pi:\mathbf{R}\to\mathbf{C}$ 连续. 因此 $\mathbf{T}$ 上的连续函数空间 $\mathscr{C}(\mathbf{T})$ 等同于 $\mathbf{R}$ 上周期为 1 的连续函数空间.

$\mathbf{T}$ 是一个群 (是交换群 $(\mathbf{R},+)$ 对于其子群 $\mathbf{Z}$ 的商), 而且由构造知, $\pi:\mathbf{R}\to\mathbf{T}$ 是一个核为 $\mathbf{Z}$ 的群态射. 如果 $n\in\mathbf{Z}$, 则 $t\mapsto e^{2i\pi nt}$ 是 $\mathbf{R}$ 的一个连续特征标, 它的核包含了 $\mathbf{Z}$, 于是由于在周期为 1 的周期函数与 $\mathbf{T}$ 上函数的等同性, 故它是 $\mathbf{T}$ 的一个连续特征标. 以 χ_n 记 $\mathbf{T}$ 的特征标 $t\mapsto e^{2i\pi nt}$, 其中 $n\in\mathbf{N}$.

命题 IV.3.1. — $\mathbf{T}$ 的连续线性特征标是 χ_n, $n\in\mathbf{N}$.

证明 如果 $\chi:\mathbf{T}\to\mathbf{C}^*$ 是一个连续线性特征标, 则 $\psi=\chi\circ\pi$ 是 $\mathbf{R}$ 的一个特征标, 它是周期为 1 的周期函数, 根据命题 IV.2.1, 存在 $\lambda\in\mathbf{C}$ 使得 $\psi(t)=e^{\lambda t}$, 其中 $t\in\mathbf{R}$. 于是 ψ 的周期性等价于 $\psi(1)=\psi(0)=1$. 这证明了 λ 应具有 $2i\pi n$ 的形式, 其中 $n\in\mathbf{N}$. 得证. □

如果 $a\in\mathbf{R}$, 则 $\mathbf{R}$ 的每个元 t 都可以写成 $t=x+n$ 的形式, 其中 $x\in[a,a+1[$, 而 $n\in\mathbf{Z}$. 换而言之, 区间 $[a,a+1[$ 是 $\mathbf{R}$ mod $\mathbf{Z}$ 的一个代表系, 其中 $a\in\mathbf{R}$ 任意. 由此知将 $\mathbf{T}$ 上函数 f 映到它在 $[a,a+1[$ 上的限制的映射 ι_a (更准确地说, 是 $f\circ\pi$ 的限制) 是一个从 $\mathbf{T}$ 上的函数空间到 $[a,a+1[$ 上的函数空间的一个同构. 我们马上要利用这个同构定义 $\mathbf{T}$ 上的一些函数空间.

利用勒贝格积分对于平移的不变性容易证明下面对于 $f:\mathbf{T}\to\mathbf{C}$ 的一些定义不依赖 $a\in\mathbf{R}$ 的选取.

称 f 为几乎处处为 0 是说 $\iota_a(f)$ 几乎处处为 0.

称 f 为可和的是说 $\iota_a(f)$ 为可和的; 如果 f 可和, 则定义 $\int_{\mathbf{T}}f$ 为 $\int_{\mathbf{T}}f=\int_a^{a+1}f(t)dt$, 且 $\|f\|_1$ 为 $\|f\|_1=\int_{\mathbf{T}}|f|$.

称 f 为平方可和的是说 $\iota_a(f)$ 平方可和; 如果 f 平方可和, 则令 $\|f\|_2=(\int_{\mathbf{T}}|f|^2)^{1/2}$, 而如果 f,g 均平方可和, 则定义它们的标量积 $\langle f,g\rangle$ 为 $\langle f,g\rangle=\int_{\mathbf{T}}\bar{f}g$.

以 $\mathscr{L}^1(\mathbf{T})$(分别地, $\mathscr{L}^2(\mathbf{T})$) 记可和 (分别地, 平方可和) 的函数空间, 而 $L^1(\mathbf{T})$ (分别地, $L^2(\mathbf{T})$) 代表前面的空间对于几乎处处为零的函数空间的商空间. 由定义知, 这些空间 (通过 ι) 分别同构于空间 $\mathscr{L}^1([a,a+1[)$, $\mathscr{L}^2([a,a+1[)$, $L^1([a,a+1[)$ 和
[337] $L^2([a,a+1[)$. 由于 $[a,a+1[$ 具有限体积, 故 $L^2(\mathbf{T})\subset L^1(\mathbf{T})$.

定义 $\mathrm{Esc}(\mathbf{T})$ 为 $\mathrm{Esc}([0,1[)$ 在 ι_0 下的逆像; 如果 $r\in\mathbf{N}$, 且若 $k\in\{0,\ldots,2^r-1\}$, 则也以 $e_{r,k}$ 记 $\mathbf{T}$ 上的其在 ι_0 下的像为 $e_{r,k}$ 的函数. 这些 $e_{r,k}$, $r\in\mathbf{N}$, $k\in\{0,\ldots,2^r-1\}$ 的函数构成了 $\mathrm{Esc}(\mathbf{T})$ 的一个生成族. 又, $\mathrm{Esc}(\mathbf{T})$ 在 $L^1(\mathbf{T})$ 和 $L^2(\mathbf{T})$ 中稠密: 事实上,

$\mathrm{Esc}(]0,1[)$ 在 $L^1(]0,1[)$ 和 $L^2(]0,1[)$ 中稠密 (参看定理 III.2.11).

令 $\mathrm{Trig}(\mathbf{T})$ 为三角多项式的空间 (即 χ_n 对于 $n \in \mathbf{N}$ 的线性组合).

定理 IV.3.2. — (i) $\mathrm{Trig}(\mathbf{T})$ 在 $L^2(\mathbf{T})$ 中稠密.

(ii) 对于 $n \in \mathbf{Z}$ 的 χ_n 构成 $L^2(\mathbf{T})$ 的一个希尔伯特基.

证明 我们有

$$\langle \chi_n, \chi_m \rangle = \int_a^{a+1} e^{2i\pi(m-n)t} dt = \begin{cases} 1, & m = n, \\ [\frac{1}{2i\pi(m-n)} e^{2i\pi(m-n)t}]_a^{a+1} = 0, & m \neq n. \end{cases}$$

因此 χ_n 构成了一个法正交族, 由于 χ_n 生成了 $\mathrm{Trig}(\mathbf{T})$, 故 (ii) 是 (i) 的推论. 证明 $\mathrm{Trig}(\mathbf{T})$ 在 $L^2(\mathbf{T})$ 中稠密的标准方法 (参看习题 II.2.2) 是通过它在 $\mathscr{C}(\mathbf{T})$ 的稠密性得到 (是斯通 – 魏尔斯特拉斯定理的特殊情形). 我给出下面的通过阶梯函数的另一个方法.

设 F 是 $\mathrm{Trig}(\mathbf{T})$ 在 $L^2(\mathbf{T})$ 中的闭包. 后面的引理 IV.3.3 表明由当 $t \in [\frac{-1}{2}, \frac{1}{2}[$ 时 $\phi_0(t) = t$ 定义的函数 $\phi_0 \in L^2(\mathbf{T})$ 有 $\phi_0 \in F$. 我们由此将可推出 F 包含了 $\mathrm{Esc}(\mathbf{T})$, 从而可以证明这个空间在 $L^2(\mathbf{T})$ 中稠密.

令 $T_a : L^2(\mathbf{T}) \to L^2(\mathbf{T})$ 为 $(T_a(\phi))(t) = \phi(t+a)$. 由于 T_a 积分在平移下的不变性, T_a 便是一个等距映射; 特别地, T_a 连续. 又由于 $\mathrm{Trig}(\mathbf{T})$ 在 T_a 下稳定, 故 F 也稳定 [如果 $\phi \in F$ 而 $(f_n)_{n\in\mathbf{N}}$ 为 $\mathrm{Trig}(\mathbf{T})$ 中的序列, 它在 $L^2(\mathbf{T})$ 中趋向 ϕ, 那么 $(T_a(f_n))_{n\in\mathbf{N}}$ 在 $L^2(\mathbf{T})$ 中趋向 $T_a(\phi)$]. 现在, 如果 $r \in \mathbf{N}$, 而 $k \in \{0, \ldots, 2^r - 1\}$, 则通过简单的计算有 $e_{r,k} = 2^{-r} - T_{-\frac{1}{2}-\frac{k}{2^r}}(\phi_0) + T_{-\frac{1}{2}-\frac{k+1}{2^r}}(\phi_0)$; 因此从 ϕ_0 属于 F 以及在 F 上为常值, 得到 $e_{r,k}, r \in \mathbf{N}, k \in \{0, \ldots, 2^r - 1\}$ 也如此. 这些 $e_{r,k}$ 构成了 $\mathrm{Esc}(\mathbf{T})$ 的一个生成元族, 从而表明 $\mathrm{Esc}(\mathbf{T}) \subset F$, 这即为所证. □

引理 IV.3.3. — (i) 如果 $t \in]\frac{-1}{2}, \frac{1}{2}[$, 而 $z = e^{2i\pi t}$, 则 $\sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{2i\pi n}(z^n - \bar{z}^n) = t$,

(ii) 级数 $\sum_{n\neq 0} \frac{(-1)^{n-1}}{2i\pi n} e^{2i\pi nt}$ 在 $L^2(\mathbf{T})$ 中趋向 ϕ_0.

证明 如果 $|a| = 1$ 且 $a \neq -1$, 则有

$$\sum_{n=1}^{N} \frac{(-1)^{n-1}}{2i\pi n} a^n = \frac{a}{2i\pi} \int_0^1 \sum_{n=1}^{N} (-ua)^{n-1} du = \frac{a}{2i\pi} \int_0^1 \frac{1-(-ua)^N}{1+ua} du.$$

由于 $|a| = 1$, 函数序列 $\frac{1-(-ua)^N}{1+ua}$, $N \in \mathbf{N}$ 在 $[0,1[$ 上单趋向 $\frac{1}{1+ua}$, 并且其模被 $\frac{2}{|1+ua|}$ [338] 控制, 但由于 $a \neq -1$, 这个强函数是可和的. 那么利用控制收敛定理得极限与积分的交换. 由此得到我们所关注的级数收敛于

$$\frac{z}{2i\pi} \int_0^1 \frac{du}{1+uz} - \frac{\bar{z}}{2i\pi} \int_0^1 \frac{du}{1+u\bar{z}} = \frac{1}{\pi} \int_0^1 \frac{\sin 2\pi t}{(u+\cos 2\pi t)^2 + \sin^2 2\pi t} du$$

$$= \frac{1}{\pi} [\arctan \frac{u+\cos 2\pi t}{\sin 2\pi t}]_0^1 = \frac{1}{\pi} (\arctan(\cot \pi t) - \arctan(\cot 2\pi t)) = t,$$

其中用到, 当 $0 < x < \pi$ 时 $\arctan(\cot x) = \frac{\pi}{2} - x$, 而当 $-\pi < x < 0$ 时等于 $\frac{-\pi}{2} - x$. (i) 得证. 现在, $\sum_{n\neq 0} \frac{1}{4\pi^2 n^2} < +\infty$, 且由于这些 χ_n 构成了一个法正交族, 故根据引理 II.2.4, 级数 $\sum_{n\neq 0} \frac{(-1)^{n-1}}{2i\pi n}\chi_n$ 在 $L^2(\mathbf{T})$ 可和. 以 f 记它的和. 于是可以从它的部分和的序列中抽出一个几乎处处趋向 f 的子序列 (参看习题 III.2.9). 但是 (i) 已经证明在 $\frac{1}{2}$ 外它的部分和的子序列均单收敛于 ϕ_0. 由此得到几乎处处 $f = \phi_0$, 从而该级数在 $L^2(\mathbf{T})$ 中趋向 ϕ_0. 证完. □

如果 $f \in L^1(\mathbf{T})$, 记 $c_n(f) = \langle \chi_n, g\rangle = \int_0^1 e^{-2i\pi nt} f(t)dt$ 为它的第 n 个傅里叶系数.

推论 IV.3.4. — 如果 $f \in L^2(\mathbf{T})$, 则 $\sum_{n\in\mathbf{Z}} c_n(f)\chi_n$ 可和, 其在 $L^2(\mathbf{T})$ 中的和为 f, 且 $\|f\|_2 = (\sum_{n\in\mathbf{Z}} |c_n(f)|^2)^{1/2}$.

证明 是定理 II.2.6 的简单应用. □

习题 IV.3.5. — 以两种方式计算 $\|\phi_0\|_2$. 由此推出 $\zeta(2) = \frac{\pi^2}{6}$.

命题 IV.3.6. — 如果 $f \in \mathscr{C}(\mathbf{T})$, 且 $\sum_{n\in\mathbf{Z}} |c_n(f)| < +\infty$, 则 $\sum_{n\in\mathbf{Z}} c_n(f)\chi_n$ 一致趋向 f. 特别地, 对每个 t 有 $f(t) = \sum_{n\in\mathbf{Z}} c_n(f)e^{2i\pi nt}$.

证明 级数 $\sum_{n\in\mathbf{Z}} c_n(f)\chi_n$ 在 $\mathscr{C}(\mathbf{T})$ 中按范数收敛 (赋以范数 $\|\ \|_\infty$), 因而其和 g 是一个连续函数. 另外, 由推论 IV.3.4 知, 此级数也在 $L^2(\mathbf{T})$ 中趋向 f, 从而在 $L^2(\mathbf{T})$ 中 $f = g$. 这就是说 $\int_0^1 |f(t) - g(t)|^2 dt = 0$, 加之 f 和 g 连续, 故意味着 $f - g$ 恒等于 0. 得证. □

注记 IV.3.7. — 条件 $\sum_{n\in\mathbf{Z}} |c_n(f)| < +\infty$ 特别当 f 属于 $\mathscr{C}^1$ 时满足. 事实上, 如果 $n \neq 0$, 分部积分给出了

$$c_n(f) = \int_0^1 f(t)e^{-2i\pi nt}dt = \frac{1}{2i\pi n}\int_0^1 f'(t)e^{-2i\pi nt}dt = \frac{1}{2i\pi n}c_n(f'),$$

[339] 且由于 $(\sum_{n\neq 0} |c_n(f')|^2)^{1/2} \leqslant \|f'\|_2$, 有

$$\sum_{n\neq 0} |\frac{1}{2i\pi n}c_n(f')| \leqslant (\sum_{n\neq 0}\frac{1}{4\pi^2 n^2})^{1/2}(\sum_{n\neq 0}|c_n(f')|^2)^{1/2} < +\infty.$$

注记 IV.3.8. — 由于 $L^2([a, a+1[)$ 等距同构于 $L^2(\mathbf{T})$, 故对于 $n \in \mathbf{N}$ 的那些 χ_n 构成了 $L^2([a, a+1[)$ 的一个希尔伯特基, 又由于 $[a, a+1[$, $]a, a+1[$ 和 $[a, a+1]$ 只相差一个零测度集, 故它们也是 $L^2(]a, a+1[)$ 或者 $L^2([a, a+1])$ 的希尔伯特基. 由此非常容易得到对于所有的有限长的区间 I, 它们都是 $L^2(I)$ 的希尔伯特基.

2. 高维的傅里叶级数

对于维数 m 的傅里叶级数的研究将以十分形式化的方式归结到一维傅里叶级数的研究 [7].

2.1. 格 $\mathbf{Z}^m$ 的情形

一个函数 $f:\mathbf{R}^m\to\mathbf{C}$ 是周期为 $\mathbf{Z}^m$ 的周期函数是指, 对于所有的 $x\in\mathbf{R}^m$ 和 $\omega\in\mathbf{Z}^m$ 有 $f(x+\omega)=f(x)$. 如果是这种情形, 那么直言对于所有的 $x\in\mathbf{R}^m$ 和所有的 $j\in\{1,\dots,m\}$ 有 $f(x+e_j)=f(x)$ 就够了, 这里的 $e_1,\dots,e_m$ 是 $\mathbf{R}^m$ 的标准基.

像维数 1 的情形那样, 我们将一个周期为 $\mathbf{Z}^m$ 的周期函数看作是从群 $\mathbf{T}^m=(\mathbf{R}/\mathbf{Z})^m=\mathbf{R}^m/\mathbf{Z}^m$ 到 $\mathbf{C}$ 的一个函数, 而 $\mathbf{T}^m$ 上的连续函数空间 $\mathscr{C}(\mathbf{T}^m)$ 恒同于 $\mathbf{R}^m$ 上周期为 $\mathbf{Z}^m$ 的周期函数空间.

如果 $\boldsymbol{n}=(n_1,\dots,n_m)\in\mathbf{Z}^m$, 则以 $\chi_{\boldsymbol{n}}$ 代表 $\mathbf{T}^m$ 上定义为 $\chi_{\boldsymbol{n}}(t)=e^{2i\pi\boldsymbol{n}\cdot t}$ 的特征标.

命题 IV.3.9. — $\mathbf{T}^m$ 的连续线性特征标是所有 $\boldsymbol{n}\in\mathbf{Z}^m$ 的 $\chi_{\boldsymbol{n}}$.

证明　如果 $\chi:\mathbf{T}^m\to\mathbf{C}^*$ 是一个连续线性特征标, 那么 χ 在 $\mathbf{R}e_j$ 的限制是一个周期为 $\mathbf{Z}$ 的周期连续线性特征标, 于是根据命题 IV.3.1, 具有形式 $t_j\mapsto e^{2i\pi n_j t_j}$. 因为 $t=\sum_{j=1}^m t_je_j$, 且 χ 是一个特征标, 从而 $\chi(t)=\prod_{j=1}^m e^{2i\pi n_jt_j}=e^{2i\pi\boldsymbol{n}\cdot t}$, 其中 $\boldsymbol{n}=(n_1,\dots,n_m)$. 得到结论. □

像在一维的情形那样, 如果 $a=(a_1,\dots,a_m)\in\mathbf{R}^m$, 且 $X_a=\prod_{j=1}^m[a_j,a_j+1[$, 并定义 ι_a 为将 $\mathbf{T}^m$ 上的函数 f 带到 f 在 X_a 的限制, 则 ι_a 是一个从 $\mathbf{T}^m$ 上的函数空间到 X_a 上的函数空间的同构. 这让我们可以像一维情形那样定义 [340]

— 空间 $L^1(\mathbf{T}^m)\cong L^1(X_a)$ 和 $L^2(\mathbf{T}^m)\cong L^2(X_a)$,

— 在 $L^1(\mathbf{T}^m)$ 上的积分 $f\mapsto\int_{\mathbf{T}^m}f=\int_{X_a}f$,

— 在 $L^1(\mathbf{T}^m)$ 上的范数 $\|f\|_1=\int_{\mathbf{T}^m}|f|$,

— 在 $L^2(\mathbf{T}^m)$ 上的标量积 $(f,g)\mapsto\langle f,g\rangle=\int_{\mathbf{T}^m}\bar{f}g$, 以及与其相关的范数 $\|f\|_2=\langle f,f\rangle^{1/2}$.

勒贝格积分在平移下的不变性表明我们得到的这些定义不依赖 $a\in\mathbf{R}^m$ 的选取 (参看引理 IV.3.16 的一个更一般的陈述).

定义 $\mathrm{Esc}(\mathbf{T}^m)$ 为 $\mathrm{Esc}([0,1[^m)$ 在 ι_0 下的逆像; 如果 $r\in\mathbf{N}$ 且 $\boldsymbol{k}\in\{0,\dots,2^r-1\}^m$, 记 $e_{r,\boldsymbol{k}}$ 为 $e_{r,\boldsymbol{k}}$ 在 ι_0 下在 $\mathbf{T}^m$ 上的逆函数. 对于 $r\in\mathbf{N}$ 和 $\boldsymbol{k}\in\{0,\dots,2^r-1\}^m$ 的那

[7] 我们可以极大地借助于张量积和完备张量积来讲引理 IV.3.11 和对它的应用进行有趣的形式化. 我们已经看到 (习题 I.3.3), 如果 I 和 J 是有限的, 则在 $I\times J$ 上的函数空间是在 I 和 J 上的函数空间的张量积. 如果 I 和 J 不是有限的, 则取值要复杂得多, 但 $I\times J$ 上的某些函数空间仍旧是 I 和 J 上的函数空间的张量积. 譬如 $\mathbf{R}^m/\mathbf{Z}^m$ 上的三角多项式就是这种情形, 它是 m 个重复的 $\mathbf{R}/Z$ 上三角多项式的张量积. 至于空间 $L^2(\mathbf{R}^m/\mathbf{Z}^m)$, 则由 m 个 $L^2(\mathbf{R}/\mathbf{Z})$ 的张量积的完备化得到. 约化到一维的方法对许多问题是非常有效的.

些 $e_{r,\boldsymbol{k}}$ 构成了 $\mathrm{Esc}(\mathbf{T}^m)$ 的一个生成族.

令 $\mathrm{Trig}(\mathbf{T}^m)$ 代表 $\mathbf{T}^m$ 上的三角多项式的空间 (即对于 $\boldsymbol{n}\in\mathbf{Z}^n$ 的 $\chi_{\boldsymbol{n}}$ 的线性组合).

如果 $f\in L^1(\mathbf{T}^m)$, 对于 $\boldsymbol{n}\in\mathbf{Z}^m$ 定义 f 的傅里叶系数 $c_{\boldsymbol{n}}(f)$ 为 $c_{\boldsymbol{n}}(f)=\langle\chi_{\boldsymbol{n}},f\rangle=\int_{[0,1]^m}e^{-2i\pi\boldsymbol{n}\cdot t}f(t)dt$.

定理 IV.3.10. — (i) $\mathrm{Trig}(\mathbf{T}^m)$ 在 $L^2(\mathbf{T}^m)$ 中稠密.

(ii) 对于 $\boldsymbol{n}\in\mathbf{Z}^m$ 的 $\chi_{\boldsymbol{n}}$ 构成 $L^2(\mathbf{T}^m)$ 的一个希尔伯特基.

(iii) 如果 $f\in L^2(\mathbf{T}^m)$, 则在 $L^2(\mathbf{T}^m)$ 中有 $f=\sum_{\boldsymbol{n}\in\mathbf{Z}^m}c_{\boldsymbol{n}}(f)\chi_{\boldsymbol{n}}$.

(iv) 如果 $f\in\mathscr{C}(\mathbf{T}^m)$, 且 $\sum_{\boldsymbol{n}\in\mathbf{Z}^m}|c_{\boldsymbol{n}}(f)|<+\infty$, 则在 $\mathscr{C}(\mathbf{T}^m)$ 中有 $f=\sum_{\boldsymbol{n}\in\mathbf{Z}^m}c_{\boldsymbol{n}}(f)\chi_{\boldsymbol{n}}$, 特别地, 对于所有的 t 有 $f(t)=\sum_{\boldsymbol{n}\in\mathbf{Z}^m}c_{\boldsymbol{n}}(f)e^{2i\pi\boldsymbol{n}\cdot t}$.

证明　我们仍旧用与一维情形的类比断言来证明. 如果 $\phi_1,\ldots,\phi_m$ 为从 $\mathbf{R}$ 到 $\mathbf{C}$ 的函数, 以 $\phi_1\otimes\cdots\otimes\phi_m$ 或者更紧凑的 $\otimes_i\phi_i$ 记从 $\mathbf{R}^m$ 到 $\mathbf{C}$ 的如下定义的函数:

$$(\otimes_i\phi_i)(t)=\phi_1\otimes\cdots\otimes\phi_m(t)=\prod_{i=1}^m\phi_i(t),$$

其中 $t=(t_1,\ldots,t_m)$. 例如,

$$\chi_{\boldsymbol{n}}=\otimes_i\chi_{n_i},\ \text{其中}\ \boldsymbol{n}=(n_1,\ldots,n_m)\in\mathbf{Z}^m,$$
$$e_{r,\boldsymbol{k}}=\otimes_i e_{r,k_i},\ \text{其中}\ r\in\mathbf{N},\boldsymbol{k}=(k_1,\ldots,k_m)\in\mathbf{Z}^m.$$

引理 IV.3.11. — (i) 如果对所有的 i 几乎处处 $\phi_i=\psi_i$, 则几乎处处 $\otimes_i\phi_i=\otimes_i\psi_i$.

(ii) 如果对所有的 i, $\phi_i\in\mathscr{L}^1(\mathbf{T})$, 则 $\otimes_i\phi_i\in\mathscr{L}^1(\mathbf{T}^m)$, 并且 $\|\otimes_i\phi_i\|_1=\prod_i\|\phi_i\|_1$.

(iii) 如果对所有的 i, $\phi_i\in\mathscr{C}^2(\mathbf{T})$, 则 $\otimes_i\phi_i\in\mathscr{L}^2(\mathbf{T}^m)$, 并且 $\|\otimes_i\phi_i\|_2=\prod_i\|\phi_i\|_2$.

证明　如果 $A_i\subset\mathbf{R}$(分别地, $A\subset\mathbf{R}^m$) 为使得 $\phi_i(x)\neq\psi_i(x)$ (分别地, $\otimes_i\phi_i(x)\neq\otimes_i\psi_i(x)$) 的 x 的集合. 于是 A 包含在 $A_i\times\prod_{j\neq i}\mathbf{R}$ 的并中, 而由假设知 A_i 在 $\mathbf{R}$ 中测度为 0, 故它们在 $\mathbf{R}^m$ 中测度均为 0. (i) 得证.

[341]　(ii) 和 (iii) 是富比尼定理的直接推论. □

回到定理 IV.3.10 的证明. 上面的引理证明了映射 $(\phi_1,\ldots,\phi_m)\mapsto\otimes_i\phi_i$ 可以转移到 mod 几乎处处为零的函数的商空间上 (同时在两端取商). 由于这个映射在每个 ϕ_i 上都是线性的, 故 (ii) 和 (iii) 证明了我们如此便得到了连续的多重线性映射 $L^1(\mathbf{T})^m\to L^1(\mathbf{T}^m)$ 和 $L^2(\mathbf{T})^m\to L^2(\mathbf{T}^m)$.

要证明 $\mathrm{Trig}(\mathbf{T}^m)$ 在 $L^2(\mathbf{T}^m)$ 中稠密, 只要它的闭包包含 $\mathrm{Esc}(\mathbf{T}^m)$ 即可, 从而由线性性, 只要证明它包含那些 $e_{r,\boldsymbol{k}}$, $r\geqslant 1$, $\boldsymbol{k}\in\{0,\ldots,2^r-1\}$ 即可. 为此, 我们将 $e_{r,\boldsymbol{k}}$ 写成形式 $e_{r,\boldsymbol{k}}=\otimes_i e_{r,k_i}$, 并对每个 i 选取 $\mathrm{Trig}(\mathbf{T})$ 中的元的一个在 $L^2(\mathbf{T})$ 中趋向 e_{r,k_i} 的序列 $P_{i,n}$. 由 $(\phi_1,\ldots,\phi_m)\mapsto\otimes_i\phi_i$ 的连续性得到 $P_n=\otimes_i P_{i,n}$ 在 $L^2(\mathbf{T}^m)$ 中趋向 $e_{r,\boldsymbol{k}}$; 由于 $P_n\in\mathrm{Trig}(\mathbf{T}^m)$, 故定理的 (i) 得证.

由富比尼定理推出, 当 $\boldsymbol{n}=(n_1,\ldots,n_m)$, $\boldsymbol{\ell}=(\ell_1,\ldots,\ell_m)$ 时有 $\langle\chi_{\boldsymbol{n}},\chi_{\boldsymbol{\ell}}\rangle=\prod_{i=}^{m}\langle\chi_{n_i},\chi_{\ell_i}\rangle$, 这让我们得到了族 $\chi_{\boldsymbol{n}},\boldsymbol{n}\in\mathbf{Z}^m$ 的法正交性; 于是 (ii) 是 (i) 的推论.

(iii) 因此是定理 II.2.6 的一个应用, 而 (iv) 则像命题 IV.3.6 的证明中那样由 (iii) 推出.

证完. □

习题 IV.3.12. — 证明, 如果 $k>\frac{m}{2}$, 且 f 是属于 $\mathscr{C}^k$ 类的周期为 $\mathbf{Z}^m$ 的周期函数, 则对所有的 t 有 $f(t)=\sum_{\boldsymbol{n}\in\mathbf{Z}^m}c_{\boldsymbol{n}}(f)e^{2i\pi\boldsymbol{n}\cdot t}$.

2.2. 任意格的情形

$\mathbf{R}^m$ 的一个格 Λ 是 $\mathbf{R}^m$ 中一个形如 $\mathbf{Z}v_1+\cdots+\mathbf{Z}v_m$ 的子群, 其中 $(v_1,\ldots,v_m)$ 是 $\mathbf{R}^m$ 的一组基. 我们称 $(v_1,\ldots,v_m)$ 为 Λ 的基 (暗含是在 $\mathbf{Z}$ 上的). 最简单的例子是格 $\mathbf{Z}^m$, 它的基是 $\mathbf{R}^m$ 的标准基.

Λ 的对偶格 Λ^* 是使得对所有 $\omega\in\Lambda$ 有 $x\cdot\omega\in\mathbf{Z}$ 的 $x\in\mathbf{R}^m$ 的集合. 显然, $\mathbf{Z}^m$ 的对偶格是 $\mathbf{Z}^m$. 一般情形可由下面的引理描述.

引理 IV.3.13. — 设 $(v_1,\ldots,v_m)$ 是 Λ 的一组基, 而 A 是一个矩阵, 其 j 列是向量 v_j. 于是 $\Lambda^*={}^{\mathrm{t}}A^{-1}\mathbf{Z}^m$.

证明 $(v_1,\ldots,v_m)$ 是 Λ 的基等于 $\Lambda=A\mathbf{Z}^m=\{A\boldsymbol{n},\ \boldsymbol{n}\in\mathbf{Z}^m\}$. 然而 $x\cdot A\boldsymbol{n}={}^{\mathrm{t}}Ax\cdot\boldsymbol{n}$. 因为 $\mathbf{Z}^m$ 的对偶格是 $\mathbf{Z}^m$, 故 $x\in\Lambda^*$ 当且仅当 ${}^{\mathrm{t}}Ax\in\mathbf{Z}^m$; 换而言之, 有 $\Lambda^*={}^{\mathrm{t}}A^{-1}\mathbf{Z}^m$. □

称函数 $f:\mathbf{R}^m\to\mathbf{C}$ 是一个周期为 Λ 的周期函数是说对于所有的 $x\in\mathbf{R}^m$ 和所有的 $\omega\in\Lambda$ 有 $f(x+\omega)=f(x)$. 倘若如此, 则只要对于所有的 $x\in\mathbf{R}^m$ 和所有的 $j\in\{1,\ldots,m\}$ 有 $f(x+v_j)=f(x)$ 即可, 其中 $(v_1,\ldots,v_m)$ 是 Λ 的一组基.

通常, 我们将周期为 Λ 的周期函数看成是从群 $\mathbf{T}(\Lambda)=\mathbf{R}^m/\Lambda$ 到 $\mathbf{C}$ 的一个函数, [342] 而在 $\mathbf{T}(\Lambda)$ 上的连续函数空间 $\mathscr{C}(\mathbf{T}(\Lambda))$ 则等同于 $\mathbf{R}^m$ 上的周期为 Λ 上的连续周期函数的空间.

如果 $\omega\in\Lambda^*$, 则 $t\mapsto e^{2i\pi\omega\cdot t}$ 是 $\mathbf{R}^m$ 的一个特征标, 其核包含了 Λ; 因此是 $\mathbf{T}(\lambda)$ 的一个特征标, 记其为 χ_ω.

引理 IV.3.14. — $\mathbf{T}(\Lambda)$ 的连续线性特征标是这些 χ_ω, $\omega\in\Lambda^*$.

证明 $\mathbf{T}(\Lambda)$ 的一个特征标具有形式 $e^{2i\pi x\cdot t}$, 其中 $x\in\mathbf{R}^m$, 其在 Λ 上为 0, 这等价于 $x\cdot\omega\in\mathbf{Z}$, 其中 $\omega\in\Lambda$. 从而得结果. □

如果 Λ 是 $\mathbf{R}^m$ 的一个格, $\mathbf{R}^m$ 的一个 mod Λ 的基本区域是指一个可测集 $X\subset\mathbf{R}^m$, 使得 $\mathbf{R}^m$ 中的每个元 x 均可以以唯一的方式写成 $\omega+a$ 的形式, 其中 $a\in X$ 而 $\omega\in\Lambda$. 例如, 如果 $(v_1,\ldots,v_m)$ 是 λ 的一组基, 则 $\{t_1v_1+\cdots+t_mv_m,\forall i,\ 0\leqslant t_i<1\}$ 是一个 mod Λ 的基本区域.

设 X 是 $\mathbf{R}^m$ 的一个 mod Λ 的基本区域. 以 $\mathrm{Vol}(\Lambda)$ 记 X 的勒贝格测度. 下面的引理 IV.3.16 证明这个定义不依赖 X 的选取; 从而, 当 $(v_1,\ldots,v_m)$ 是 Λ 的一组基时, $\mathrm{Vol}(\Lambda)=|\det(v_1,\ldots,v_m)|$; 特别地, $\mathrm{Vol}(\mathbf{Z}^m)=1$.

将 $\mathbf{T}(\Lambda)$ 上的函数 f 对应到 f 在 X 上的限制的映射 ι_X 是从 $\mathbf{T}(\Lambda)$ 上的函数空间到 X 上的函数空间的一个同构. 这让我们可以按通常那样定义:

— 空间 $L^1(\mathbf{T}(\Lambda))\cong L^1(X)$ 和 $L^2(\mathbf{T}(\Lambda))\cong L^2(X)$,

— 在 $L^1(\mathbf{T}(\Lambda))$ 中的积分 $f\mapsto\int_{\mathbf{T}(\Lambda)}f=\int_X f$,

— 在 $L^1(\mathbf{T}(\Lambda))$ 上的范数 $\|f\|_1=\frac{1}{\mathrm{Vol}(\Lambda)}\int_{\mathbf{T}(\Lambda)}|f|$,

— 在 $L^2(\mathbf{T}(\Lambda))$ 上的标量积 $(f,g)\mapsto\langle f,g\rangle=\frac{1}{\mathrm{Vol}(\Lambda)}\int_{\mathbf{T}(\Lambda)}\bar{f}g$, 并且与其相伴的范数为 $\|f\|_2=\langle f,f\rangle^{1/2}$.

后面的引理 IV.3.16 将证明我们所得到的这些都不依赖 X 的选取.

如果 $f\in L^1(\mathbf{T}(\Lambda))$, 定义它的傅里叶系数 $c_\omega(f)$, $\omega\in\Lambda^*$ 为 $c_\omega(f)=\langle\chi_\omega,f\rangle=\frac{1}{\mathrm{Vol}(\Lambda)}\int_X e^{-2i\pi\omega\cdot t}f(t)dt$, 其中的 X 是 Λ 的一个基本区域.

定理 IV.3.15. — (i) 对于 $\omega\in\Lambda^*$ 的这些 χ_ω 构成了 $L^2(\mathbf{T}(\Lambda))$ 一个希尔伯特基.

(ii) 如果 $f\in L^2(\mathbf{T}(\Lambda))$, 则在 $L^2(\mathbf{T}(\Lambda))$ 中 $f=\sum_{\omega\in\Lambda^*}c_\omega(f)\chi_\omega$.

(iii) 如果 $f\in\mathscr{C}(\mathbf{T}(\Lambda))$, 且 $\sum_{\omega\in\Lambda^*}|c_\omega(f)|<+\infty$, 则在 $\mathscr{C}(\mathbf{T}(\Lambda))$ 中 $f=\sum_{\omega\in\Lambda^*}c_\omega(f)\chi_\omega$; 特别地, 对所有的 t 有 $f(t)=\sum_{\omega\in\Lambda^*}c_\omega(f)e^{2i\pi\omega\cdot t}$.

证明　设 $(v_1,\ldots,v_m)$ 是 Λ 的一组基, 并设 A 为其 j 列为 v_j 的矩阵. 于是 $A\cdot\mathbf{Z}^m=\Lambda$, 这使得 $\phi\mapsto\phi\circ A$ 将周期为 Λ 的周期函数映成周期为 $\mathbf{Z}^m$ 的周期函数. 另外, 在 $L^2(\mathbf{T}(\Lambda))$ 上标量积的定义中的因子 $\frac{1}{\mathrm{Vol}(\Lambda)}=\frac{1}{|\det A|}$ 使得 $\phi\mapsto\phi\circ A$ 成为从 $L^2(\mathbf{T}(\Lambda))$ 到 $L^2(\mathbf{T}^m)$ 上的等距映射. 注意到, 当 $\omega={}^tA^{-1}\boldsymbol{n}\in\Lambda^*$(见引理 IV3.13) 时有 $\chi_\omega(At)=\chi_{\boldsymbol{n}}(t)$, 于是这让我们从关于 $\mathbf{Z}^m$ 的结果推导出了此定理. [343] □

引理 IV.3.16. — 如果 $f:\mathbf{T}(\Lambda)\to\mathbf{R}_+$ 可测, 则 $\int_X f$ 不依赖 Λ 的基本区域 X 的选取.

证明　X 为 mod Λ 的基本区域表明它可以写成为 $\sum_{\omega\in\Lambda}\mathbf{1}_{\omega+X}=1$ 的形式, 其中 $\omega+X=\{\omega+a,a\in X\}$

设 X_1,X_2 为 mod Λ 的基本区域. 在下面逐次地利用:

— 恒等式 $1=\sum_{\omega\in\Lambda}\mathbf{1}_{\omega+X_2}$,

— 单调收敛定理以交换和与积分,

— 变量变换 $x=\omega+t$ 以及在变量变换下 f 的不变性,

— 又一次的单调收敛定理,

— 恒等式 $\sum_{\omega\in\Lambda}\mathbf{1}_{-\omega+X_1}=1$, 便得到

$$\int_{X_1}f=\int\mathbf{1}_{X_1}f=\int(\sum_{\omega\in\Lambda}\mathbf{1}_{\omega+X_2})\mathbf{1}_{X_1}f=\sum_{\omega\in\Lambda}\int\mathbf{1}_{\omega+X_2}\mathbf{1}_{X_1}f$$

$$= \sum_{\omega\in\Lambda} \int \mathbf{1}_{X_2}\mathbf{1}_{-\omega+X_1} f = \int (\sum_{\omega\in\Lambda} \mathbf{1}_{-\omega+X_1})\mathbf{1}_{X_2} f = \int \mathbf{1}_{X_2} f = \int_{X_2} f,$$

故得证. □

3. 泊松公式

以 $\mathscr{S}(\mathbf{R}^m)$ 记 $\mathbf{R}^m$ 上属于 $\mathscr{C}^\infty$ 类的, 并在无限远连同其所有导数速降的函数的施瓦兹空间. (g 在无限远速降是说, 对于任意的 $N\in\mathbf{N}$, $(1+\|t\|^2)^N g(t)$ 在 $\mathbf{R}^m$ 上有界.) 由定理 IV.2.8 可推出下面的结果.

推论 IV.3.17. — $\mathscr{S}(\mathbf{R}^m)$ 在傅里叶变换下的像包含在 $\mathscr{S}(\mathbf{R}^m)$ 中.

定理 IV.3.18. — (泊松公式, 1816) 如果 $f\in\mathscr{S}(\mathbf{R})$, 或者更一般地, 如果 f 属于 $\mathscr{C}^1$, 并且若 f 和 f' 在 $\pm\infty$ 是 $O(|t|^{-2})$ 的, 则

$$\sum_{n\in\mathbf{Z}} f(n) = \sum_{n\in\mathbf{Z}} \hat{f}(n).$$

证明　设 $F(t)=\sum_{n\in\mathbf{Z}} f(n+t)$. 由于假设了 $f=O(|t|^{-2})$, 此级数对于所有的 t 收敛, 并且函数 F 是周期 1 的周期函数. 又由于按假设 $f'=O(|t|^{-2})$, 故在 $[0,1]$ 上 $f'(n+t)$ 的级数按范数收敛, 这表明 $F\in\mathscr{C}^1(\mathbf{T})$. 由此并利用注记 IV.3.7 得到 F 在每点是它的傅里叶级数的和. 然而, 如果 $k\in\mathbf{Z}$, 我们有 (下面的积分和级数的互换的 [344] 合理性来自在 $[0,1]$ 上的一致收敛性):

$$c_k(F) = \int_0^1 e^{-2i\pi kt}F(t)dt = \int_0^1 e^{-2i\pi kt}(\sum_{n\in\mathbf{Z}} f(n+t))dt = \sum_{n\in\mathbf{Z}} \int e^{-2i\pi kt} f(n+t)dt$$
$$= \sum_{n\in\mathbf{Z}} \int_n^{n+1} e^{-2i\pi kt} f(t)dt = \int_{-\infty}^{+\infty} e^{-2i\pi kt} f(t)dt = \hat{f}(k).$$

比较给出 $F(0)$ 的级数与 F 在 0 的傅里叶级数, 便由此得到定理的公式. □

我们同样可以证明在任意维数情形有下述结果.

定理 IV.3.19. — ($\mathbf{R}^m$ 中的泊松公式) 如果 $f\in\mathscr{S}(\mathbf{R}^m)$, 而 Λ 是 $\mathbf{R}^m$ 的一个格, 则

$$\sum_{\omega\in\Lambda} f(\omega) = \frac{1}{\mathrm{Vol}(\Lambda)} \sum_{\omega\in\Lambda^*} \hat{f}(\omega).$$

习题 IV.3.20. — 比较给出定理 IV.3.18 的公式与定理 IV3.19 的公式的值 $\sum_{n\in\mathbf{Z}} f(\lambda n)$, 其中 $\lambda\in\mathbf{R}^*$.

4. 在 $\mathscr{S}$ 中的傅里叶反演公式

定理 IV.3.21. — 如果 $\varphi\in\mathscr{S}(\mathbf{R}^m)$, 则 $\overline{\mathscr{F}}\mathscr{F}\varphi=\varphi$, 且 $\mathscr{F}\overline{\mathscr{F}}\varphi=\varphi$.

注记 IV.3.22. — 由于 $\overline{\mathscr{F}}\varphi(x) = \mathscr{F}\varphi(-x)$, 故可重写公式 $\overline{\mathscr{F}}\mathscr{F}\varphi = \varphi$ 为 $(\mathscr{F} \circ \mathscr{F}\varphi)(x) = \varphi(-x)$ 或者 $\hat{\hat{\varphi}} = \varphi(-x)$.

证明 由于将 x 变为 $-x$ 时便从 $\mathscr{F}$ 转移到了 $\overline{\mathscr{F}}$, 故只需证明两个公式中的一个即可. 我们证明第一个. 设 $u \in \mathbf{R}^m$, 而 $r \in \mathbf{N}$. 如果将泊松公式用于函数 $f(t) = \varphi(u+2^r t)$ 和格 $\Lambda = \mathbf{Z}^m$ (其中 $\Lambda^* = \mathbf{Z}^m$)(在这里我们利用恒等式 $\hat{f}(x) = 2^{-rm}e^{2i\pi u\cdot 2^{-r}x}\hat{\varphi}(2^{-r}x)$, 它是伸缩 – 平移公式的结果):

$$\sum_{\boldsymbol{k}\in\mathbf{Z}^m} \varphi(u + 2^r\boldsymbol{k}) = 2^{-rm} \sum_{\boldsymbol{k}\in\mathbf{Z}^m} e^{2i\pi u\cdot 2^{-r}\boldsymbol{k}}\hat{\varphi}(2^{-r}\boldsymbol{k}).$$

我们要证明, 当 $r \to +\infty$ 时, 上式左端趋向 $\varphi(u)$, 而右端趋向 $\overline{\mathscr{F}}\hat{\varphi}(u)$, 这便得到结论.

• 首先注意, 由于 φ 在无限远趋向 0, 故当 $\boldsymbol{k} \neq 0$ 时有 $\varphi(u + 2^r\boldsymbol{k}) \to 0$, 而当 $\boldsymbol{k} = 0$ 时有 $\varphi(u + 2^r\boldsymbol{k}) = \varphi(u)$; 为了证明左端的项趋向 $\varphi(u)$, 因此只要验证求和与取极限可互换即可. φ 在无限远的速降性特别表明存在 C 使得对于 $t \in \mathbf{R}^m$ 有 $|\varphi(t)| \leqslant C(1 + \|t\|^2)^{-(m+1)/2}$. 然而对于每一个 $a > 0, \sum_{\boldsymbol{k}\in\mathbf{Z}^m}(1 + a\|k\|^2)^{-(m+1)/2} < +\infty$ (参看小词典的 15.2 小节), 以及当 $2^r \geqslant 2\|u\|$ 时有 $\|u + 2^r\boldsymbol{k}\| \geqslant a\|\boldsymbol{k}\|$, 其中的 $a = \|u\|$ 而 [345] $\boldsymbol{k} \in \mathbf{Z}^m$ 任意. 通项为 $C(1 + a\|\boldsymbol{k}\|^2)^{-(m+1)/2}$ 的级数因而对于每个充分大的 r, 是通项为 $\varphi(u + 2^r\boldsymbol{k})$ 的一个可和的控制强函数. 对这些级数利用控制收敛定理便可得结论.

• 转到对右端的级数的研究. 将一个和转换为一个阶梯函数的积分的通常做法证明这个级数等于 $\int \psi_r$, 其中 ψ_r 是由

$$\psi_r = \sum_{\boldsymbol{k}\in\mathbf{Z}^m} \psi(2^{-r}\boldsymbol{k})e_{r,\boldsymbol{k}}, \text{ 而 } \psi(x) = e^{2i\pi u\cdot x}\hat{\varphi}(x)$$

定义的函数. 现在, 如果 $t = (t_1, \ldots, t_m)$, 则 $\psi_r(t) = \psi(t^{(r)})$, 其中 $t_i^{(r)} = 2^{-r}[2^r t_i] \in [t_i - 2^{-r}, t_i]$. 特别地, 对于 $t^{(r)} \to t$ 和连续的 ψ, 以及所有的 $t \in \mathbf{R}^m$, 我们有 $\psi_r(t) \to \psi(t)$. 另外, 如果 $C(t)$ 代表方体 $\prod_{i=1}^m [t_i - 1, t_i]$, 则对于每个 $r \in \mathbf{N}$ 有 $t^{(r)} \in C(t)$. 因此函数 ψ_r 对于每个 $r \in \mathbf{N}$ 均被强函数 g 控制, 这里的 g 为 $g(t) = \sup_{u\in C(t)} |\psi(t)| = \sup_{u\in C(t)} |\hat{\varphi}(t)|$. 最后, 由于 $\hat{\varphi}$ 是在无限远速降的函数, 故 g 也同样如此, 故而知其可和; 这使得我们可利用控制收敛定理证明 $\int \psi_r \to \int \psi$. 因为 $\int \psi = \overline{\mathscr{F}}\hat{\varphi}(u)$, 故得结论. □

推论 IV.3.23. — $\mathscr{F}$ 和 $\overline{\mathscr{F}}$ 是 $\mathscr{S}(\mathbf{R}^m)$ 和 $\mathscr{S}(\mathbf{R}^m)$ 间相互为逆的同构[8].

5. 在 L^1 中的反演公式

命题 IV.3.24. — 如果 $f, g \in L^1(\mathbf{R}^m)$, 则

$$\int_{\mathbf{R}^m} g\mathscr{F}f = \int_{\mathbf{R}^m} f\mathscr{F}g \quad \text{和} \quad \int_{\mathbf{R}^m} g\overline{\mathscr{F}}f = \int_{\mathbf{R}^m} f\overline{\mathscr{F}}g.$$

[8] 这个结果再结合上命题 IV.3.24 是定义分布 (或广义函数) 的傅里叶变换的基础.

证明　注意, 由于 $\hat{f}$, $\hat{g}$ 都是 $\mathscr{C}_0(\mathbf{R}^m)$ 中的元从而有界, 故上面公式的两端均有定义. 令 $h(x,t)=g(x)f(t)e^{-2i\pi x\cdot t}$. 于是由关于正函数的富比尼定理知 h 在 $\mathbf{R}^m\times\mathbf{R}^m$ 上可和, 因此有

$$\int_{\mathbf{R}^m\times\mathbf{R}^m}|h(x,t)|dxdt=\int_{\mathbf{R}^m\times\mathbf{R}^m}|f(t)||g(x)|dxdt=\int_{\mathbf{R}^m}(\int_{\mathbf{R}^m}|f(t)||g(x)|dx)dt$$
$$=\int_{\mathbf{R}^m}\|g\|_1|f(t)|dt=\|g\|_1\|f\|_1<+\infty.$$

直接应用富比尼定理便证明了这两端都等于 $\int_{\mathbf{R}^m\times\mathbf{R}^m}h(x,t)dxdt$, 故得证. □

命题 IV.3.25. — 如果 $h\in L^1(\mathbf{R}^m)$ 有一个可和的傅里叶变换, 则 $\overline{\mathscr{F}}\mathscr{F}h=h$ 几乎处处成立.

证明　设 $\varphi\in\mathscr{C}_0^\infty(\mathbf{R}^m)$. 于是根据定理 IV.3.21 有 $\mathscr{F}\overline{\mathscr{F}}\varphi=\varphi$. 另外, 逐次应用命题 IV.3.24 到 $f=\mathscr{F}h$ 和 $g=\varphi$, 然后到 $f=h$ 和 $g=\overline{\mathscr{F}}\varphi$ (因为按假设 h 和 $\mathscr{F}h$ 在 $L^1(\mathbf{R}^m)$ 中, 而 φ 和 $\overline{\mathscr{F}}\varphi$ 在 $\mathscr{S}(\mathbf{R}^m)\subset L^1(\mathbf{R}^m)$ 中, 故这样做是合理的), 于是得到 [346]

$$\int_{\mathbf{R}^m}\overline{\mathscr{F}}\mathscr{F}h\varphi=\int_{\mathbf{R}^m}\mathscr{F}h\overline{\mathscr{F}}\varphi=\int_{\mathbf{R}^m}h\mathscr{F}\overline{\mathscr{F}}\varphi=\int_{R^m}h\varphi.$$

函数 $\overline{\mathscr{F}}\mathscr{F}h$ 并不是事先就在 $L^1(\mathbf{R}^m)$ 中的, 但由于它连续, 故它在任意的有界开集 X 上的限制属于 $L^1(X)$. 然而由前面知, 对于所有的 $\varphi\in\mathscr{C}_c^\infty(X)$ 有 $\int_X(\overline{\mathscr{F}}\mathscr{F}h-h)\varphi=0$, 并且推论 III.2.13 让我们推出 $\overline{\mathscr{F}}h-h$ 在所有的有界开集 X 上几乎处处为 0. 得证. □

在下面我们将给出以习题形式出现的另一个证明 (利用在习题 III.3.12 和 III.3.13 引进的卷积), 以及在 §IV.4 的 3 小节中的另一个证明, 它被傅里叶变换转移到了 L^2 中.

习题 IV.3.26. — (反演公式)

(i) 设 $h:\mathbf{R}\to\mathbf{R}$ 由 $h(t)=e^{-|t|}$ 定义, 而 $\varepsilon>0$, 并令 $h_\varepsilon(t)=h(\varepsilon t)$, 以及 $\delta(x)=\hat{h}(-x)$.

(a) 计算 $\delta(x)$ 并证明 $\int_{\mathbf{R}}\delta=1$ 和 $\hat{h}_\varepsilon(-x)=\delta_\varepsilon(x)$, 其中 $\delta_\varepsilon(x)=\frac{1}{\varepsilon}\delta(x/\varepsilon)$.

(b) 设 $f\in L^1(\mathbf{R})$. 证明当 $\varepsilon\to 0$ 时 $\|f*\delta_\varepsilon-f\|_{L^1}\to 0$. (从 f 为阶梯函数着手.)

(c) 由此推出, 存在一个趋向 0 的序列 $(\varepsilon_n)_{n\in\mathbf{N}}$ 使得 $f*\delta_{\varepsilon_n}(x)\to f(x)$ 几乎处处对 $x\in\mathbf{R}$ 成立.

(d) 证明 $(f*\delta_\varepsilon)(x)=\int_{\mathbf{R}}h(\varepsilon t)\hat{f}(t)e^{2i\pi tx}dt$.

(ii) 又假设 $\hat{f}\in L^1(\mathbf{R})$. 令 $g(x)=\int_{\mathbf{R}}\hat{f}(t)e^{2i\pi tx}dt$. 证明 g 有界, 连续, 以及当 $\varepsilon\to 0$ 时对任意的 $x\in\mathbf{R}$ 有 $\int_{\mathbf{R}}h(\varepsilon t)\hat{f}(t)e^{2i\pi tx}dt\to g(x)$. 由此得到, 对 $x\in\mathbf{R}$ 有 $f(x)=g(x)$ 几乎处处成立.

6. 习题

习题 IV.3.27. — 设 $f:\mathbf{R}\to\mathbf{C}$ 由 $f(t)=\frac{1}{(t+i)^3}$ 定义.

(i) 证明 $\hat{f}$ 有定义, 且属于 $\mathscr{C}^1$, 以及对于每个 $N\in\mathbf{N}$, 当 $|t|\to+\infty$ 时有 $|t^N\hat{f}(t)|\to 0$.

(ii) 设 $g:\mathbf{R}\to\mathbf{C}$ 的定义为: 当 $t>0$ 时 $g(t)=e^{-2\pi t}$, 而当 $t\leqslant 0$ 时 $g(t)=0$. 计算 $\hat{g}$; 并由此得出 $h(t)=t^2g(t)$ 的傅里叶变换, 然后得出 $\hat{f}$.

(iii) 证明级数 $\sum_{n\in\mathbf{Z}}\frac{1}{(n+i)^3}$ 绝对收敛, 并计算其和.

习题 IV.3.28. — (i) 证明, 如果 $\phi\in\mathscr{C}_c^\infty$, 则微分方程 $u''-u=\phi$ 在 $\mathscr{S}(\mathbf{R})$ 中有唯一的解. 它总是具有紧支集吗?

(ii) 在 $\hat{\phi}$ 上加上什么条件可使微分方程 $u''+u=\phi$ 在 $\mathscr{S}(\mathbf{R})$ 中有解? 如果其有解, 它是否总具有紧支集?

习题 IV.3.29. — 设 $f:\mathbf{R}\to\mathbf{R}$ 由 $f(t)=e^{-\pi t^2}$ 定义.

(i) 证明 $\hat{f}$ 在 $\mathbf{R}$ 上属于 $\mathscr{C}^\infty$, 并满足微分方程 $\hat{f}'(x)=-2\pi x\hat{f}(x)$. 利用公式 $\int_{\mathbf{R}}e^{-\pi t^2}dt=1$ 由此推导出 $\hat{f}(x)=e^{-\pi x^2}$.

(ii) 如果 $u\in\mathbf{R}_+^*$, 计算 f_u 的傅里叶变换, 其中 $f_u(t)=e^{-\pi ut^2}$.

(iii) 如果 $u\in\mathbf{R}_+^*$, 且 $F(u)=\sum_{n\in\mathbf{Z}}e^{-\pi n^2u}$, 证明 $F(u)=\frac{1}{\sqrt{u}}F(\frac{1}{u})$.

[347] **习题 IV.3.30.** — 如果 $\lambda>0$, 并设 $\phi_\lambda(t)=e^{-\pi\lambda|t|}\frac{\sin\pi t}{\pi t}$.

(i) 证明 $\lambda\mapsto\hat{\phi}_\lambda(x)$, $x\in\mathbf{R}$ 在 $\mathbf{R}_+^*$ 上可导. 计算 $\hat{\phi}_\lambda(x)$.

(ii) 注意到 $\frac{\sin\pi t}{\pi t}$ 是 $\mathbf{1}_{[\frac{-1}{2},\frac{1}{2}[}$ 的傅里叶变换, 从而直接重新证明 (i).

IV.4. 在 L^2 中的傅里叶变换

如果 $\phi\in L^2(\mathbf{R}^m)$ 不是可和的, 于是积分 $\int_{\mathbf{R}^m}e^{-2i\pi xt}\phi(t)dt$ 对于任何一个 x 的值不收敛. 尽管有这个小问题, 我们还是可以通过取极限的办法定义 $L^2(\mathbf{R}^m)$ 中的一个元的傅里叶变换, 而我们得到的却给出了一个比在 $L^1(\mathbf{R}^m)$ 的情形具有更好性质的理论. 有许多的方式可以到达此结果. 而我们始终优先选择用阶梯函数的方法. 在问题 H.6 中还将找到另一个方式.

1. 阶梯函数的傅里叶变换

先对一维的情形进行一些计算.

引理 IV.4.1. — (i) 如果 $\lambda>0$, 则 $e^{-\pi\lambda|t|}\frac{\sin\pi t}{\pi t}$ 的傅里叶变换是

$$\frac{1}{\pi}(\arctan(\frac{2x+1}{\lambda})-\arctan(\frac{2x-1}{\lambda})).$$

(ii) $\frac{\sin^2 \pi t}{(\pi t)^2}$ 的傅里叶变换是 $\frac{1}{2}(|x+1|+|x-1|-2|x|)$.

证明 (i) 我们来计算 $\int_{\mathbf{R}} e^{-2i\pi xt}e^{-\pi\lambda|t|}\frac{\sin \pi t}{\pi t}dt$. 但 $\frac{\sin \pi t}{\pi t}$ 是 $\mathbf{1}_{[\frac{-1}{2},\frac{1}{2}[}$ 的傅里叶变换, 而 $e^{-2i\pi xt}e^{-\pi\lambda|t|}$ 的傅里叶变换是

$$y \mapsto \int_{\mathbf{R}} e^{-2i\pi(x+y)t}e^{-\pi\lambda|t|}dt = \int_0^{+\infty} e^{-\pi t(\lambda+2i(x+y))}+e^{-\pi t(\lambda-2i(x+y))}dt$$

$$= \frac{1}{\pi}(\frac{1}{\lambda+2i(x+y)}+\frac{1}{\lambda-2i(x+y)} = \frac{2\lambda}{\pi(\lambda^2+4(x+y)^2)}.$$

因此由命题 IV.3.24 得到 $\int_{\mathbf{R}} e^{-2i\pi xt}e^{-\pi\lambda|t|}\frac{\sin \pi t}{\pi t}dt = \int_{\frac{-1}{2}}^{\frac{1}{2}} \frac{2\lambda}{\pi(\lambda^2+4(x+y)^2)}dy$. 利用 $\frac{2\lambda}{\pi(\lambda^2+4(x+y)^2)}$ 的原函数为 $\frac{1}{\pi}\arctan(\frac{2(x+y)}{\lambda})$ 便得到了结果.

(ii) 我们将计算当 $\lambda>0$ 时 $e^{-\pi\lambda|t|}\frac{\sin^2 \pi t}{(\pi t)^2}$ 的傅里叶变换, 然后通过将 λ 趋向 0 而得到所要结果. 如果 $x\in\mathbf{R}$, 而 $\lambda\geqslant 0$; 令

$$G_x = \int_{\mathbf{R}} g_x(\lambda,t)dt,$$

其中

$$g_x(\lambda,t) = e^{-2i\pi xt}e^{-\pi\lambda|t|}\frac{\sin^2 \pi t}{(\pi t)^2}.$$

由于函数 $\frac{\sin^2 \pi t}{(\pi t)^2}$ 是对于当 $\lambda\geqslant 0$ 时 $g_x(\lambda,t)$ 的控制强函数, 又由于对于每一个 $t\geqslant 0$, $\lambda\mapsto g_x(\lambda,t)$ 在 $\mathbf{R}_+$ 上连续, 故依赖单参数的积分的连续性定理证明了 G_x 在 $\mathbf{R}_+$ 上的连续性. 于是我们所感兴趣的量 $G_x(0)$ 是当 $\lambda\to 0$ 时 $G_x(\lambda)$ 的极限.

我们可应用命题 IV.3.24 于 $G_x(\lambda)=\int_{\mathbf{R}}\hat{f}g$, 其中 $f=\mathbf{1}_{[\frac{-1}{2},\frac{1}{2}[}$, 而 $g=e^{-2i\pi xt}\cdot e^{-\pi\lambda|t|}\frac{\sin \pi t}{\pi t}$. 利用 (i), 得到 $G_x(\lambda)=\int_{\mathbf{R}}f\hat{g}=\frac{1}{\pi}\int_{-1/2}^{1/2}h_x(\lambda,y)dy$, 其中 [348]

$$h_x(\lambda,y) = \arctan(\frac{2(x+y)+1}{\lambda}) - \arctan(\frac{2(x+y)-1}{\lambda}).$$

现在, $|h_x(\lambda,y)|$ 对任意的 $\lambda>0$ 被强函数 π 控制, 而由于 $\arctan(\frac{a}{\lambda})$ 当 $\lambda\to 0^+$ 时趋向 $\mathrm{sign}(a)\frac{\pi}{2}$, 故利用单参数积分的连续性定理得到

$$G_x(0) = \frac{1}{2}\int_{-1/2}^{1/2}(\mathrm{sign}(2(x+y)+1)-\mathrm{sign}(2(x+y)-1))dy.$$

利用公式 $\int_{-1/2}^{1/2}\mathrm{sign}(2y+a)dy = |\frac{a+1}{2}|-|\frac{a-1}{2}|$ 便得到了结果. □

命题 IV.4.2. — 设 $m\geqslant 1$.

(i) 如果 $r\in\mathbf{N}$, 且 $\boldsymbol{k}\in\mathbf{Z}^m$, 则 $\hat{e}_{r,\boldsymbol{k}}\in L^2(\mathbf{R}^m)$.

(ii) 如果 $\boldsymbol{k},\boldsymbol{k}'\in\mathbf{Z}^m$, 则

$$\langle \hat{e}_{r,\boldsymbol{k}},\hat{e}_{r,\boldsymbol{k}'}\rangle = \begin{cases} 0, & \text{如果 } \boldsymbol{k}\neq\boldsymbol{k}', \\ 2^{-rm}, & \text{如果 } \boldsymbol{k}=\boldsymbol{k}' \end{cases} = \langle e_{r,\boldsymbol{k}},e_{r,\boldsymbol{k}'}\rangle.$$

(iii) 映射 $\phi \to \hat{\phi}$ 诱导了从 $\mathrm{Esc}(\mathbf{R}^m)$ 到 $L^2(\mathbf{R}^m)$ 的一个子空间上的等距同构, 这里 $\mathrm{Esc}(\mathbf{R}^m)$ 上的范数为 $\|\ \|_2$.

证明　由 $\alpha(t) = \frac{\sin \pi t}{\pi t}$ 在 $\mathbf{R}$ 上平方可积和在命题 IV.2.6 中用 α 表达出的 $\hat{e}_{r,\boldsymbol{k}}$ 的公式便推出了 (i).

通过计算立即得知 $\langle e_{r,\boldsymbol{k}}, e_{r,\boldsymbol{k}'}\rangle$ 当 $\boldsymbol{k} \neq \boldsymbol{k}'$ 时等于 0, 而当 $\boldsymbol{k} = \boldsymbol{k}'$ 时等于 2^{-rm}. 另外, 从命题 IV.2.6 中的公式

$$\hat{e}_{r,\boldsymbol{k}}(x) = \prod_{j=1}^{m} (2^{-r} e^{-2^{1-r} i\pi (k_j + \frac{1}{2}) x_j} \alpha(2^{-r} x_j))$$

出发, 便可得到 (在直接应用了富比尼定理之后)

$$\begin{aligned}\langle \hat{e}_{r,\boldsymbol{k}}, \hat{e}_{r,\boldsymbol{k}'}\rangle &= 2^{-2rm} \prod_{j=1}^{m} (\int_{\mathbf{R}} e^{-2^{1-r} i\pi (k'_j - k_j) x_j} \alpha(2^{-r} x_j)^2 dx_j) \\ &= 2^{-rm} \prod_{j=1}^{m} (\int_{\mathbf{R}} e^{-2i\pi (k'_j - k_j) u_j} \alpha(u_j)^2 du_j).\end{aligned}$$

我们认出, 在括号里的是 $\alpha^2(t) = \frac{\sin^2 \pi t}{(\pi t)^2}$ 的傅里叶变换, 这让我们可利用引理 IV.4.1 的 (ii) 来证明 $\int_{\mathbf{R}} e^{-2i\pi(k'_j - k_j)u_j} \alpha(u_j)^2 du_j$ 当 $k_j \neq k'_j$ 时为 0, 而当 $k_j = k'_j$ 时取值为 1. 从而得到 (ii).

最后, (iii) 由 (ii)(因为对于 $\boldsymbol{k} \in \mathbf{Z}^m$ 的这些 $e_{r,\boldsymbol{k}}$ 构成了 $\mathrm{Esc}_r(\mathbf{R}^m)$ 的基) 以及 $\mathrm{Esc}(\mathbf{R}^m)$ 是这些 $\mathrm{Esc}_r(\mathbf{R}^m)$, $r \in \mathbf{N}$ 的并这两个事实得到. □

[349] 2. L^2 中的傅里叶变换的定义

定理 IV.4.3. — (普朗谢雷尔 (Plancherel), 1910) $\mathscr{F} : \mathrm{Esc}(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ 可连续地延拓为从 $L^2(\mathbf{R}^m)$ 到 $L^2(\mathbf{R}^m)$ 上的等距同构, 其逆为 $\phi \mapsto \overline{\mathscr{F}}\phi$, 其中 $\overline{\mathscr{F}}\phi(x) = \mathscr{F}\phi(-x)$.[9] 换而言之, 就是:

(i) 如果 $\phi_1, \phi_2 \in L^2(\mathbf{R}^m)$, 则 $\langle \mathscr{F}\phi_1, \mathscr{F}\phi_2\rangle = \langle \phi_1, \phi_2\rangle$($\mathscr{F}$ 是一个等距映射).

(ii) 如果 $\phi \in L^2(\mathbf{R}^m)$, 则 $\mathscr{F}(\mathscr{F}\phi)(x) = \phi(-x)$ (L^2 中的傅里叶反演公式).

另外, IV.2.2 小节中对于伸缩, 平移和乘以特征标的公式在 $L^2(\mathbf{R}^m)$ 中仍然成立, 并且, 如果 $\phi \in L^1(\mathbf{R}^m) \cap L^2(\mathbf{R}^m)$, 则 $\mathscr{F}\phi$ 的这两个定义相合.

证明　由命题 IV.4.2 和 $\mathrm{Esc}(\mathbf{R}^m)$ 在 $L^2(\mathbf{R}^m)$ 中的稠密性得知, $\mathscr{F}$ 可以以唯一的方式延拓为从 $L^2(\mathbf{R}^m)$ 到 $L^2(\mathbf{R}^m)$ 的一个子空间上的等距同构[10]. 另外, 对于伸缩, 平移和乘以一个特征标也由连续性扩张到了 $L^2(\mathbf{R}^m)$.

---

[9] 写成 $\phi(x)$ 有点滥用记号之嫌; 为了正确书写, 最好写成 $\overline{\mathscr{F}} = \mathscr{F} \circ s$, 其中 $s : L^2(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ 是对在 $\mathscr{L}^2(\mathbf{R}^m)$ 上由 $s(\phi)(x) = \phi(-x)$ 定义的映射转移到商空间得到的.

[10] 由于维数是无穷的, 故映射的单性并不表明就已经意味着它的满性.

现在, 如果 $\phi \in L^1(\mathbf{R}^m) \cap L^2(\mathbf{R}^m)$, 以 $\mathscr{F}_1\phi$(分别地, $\mathscr{F}_2\phi$)(暂时地) 记 ϕ 在 $L^1(\mathbf{R}^m)$(分别地, $L^2(\mathbf{R}^m)$) 中的傅里叶变换. 设 $(f_j)_{j\in\mathbf{N}}$ 为 $\mathrm{Esc}(\mathbf{R}^m)$ 中的序列, 它同时在 $L^1(\mathbf{R}^m)$ 和 $L^2(\mathbf{R}^m)$ 中收敛于 ϕ (参看定理 III.2.11). 于是 $\mathscr{F}_1 f_j = \mathscr{F}_2 f_j$ 一致地趋向连续函数 $\mathscr{F}_1\phi$, 并在范数 $\|\ \|_2$ 下趋向 $\mathscr{F}_2\phi$. 根据引理 III.2.14, 这表明 $\mathscr{F}_1\phi \in L^2(\mathbf{R}^m)$, 并且几乎处处 $\mathscr{F}_1\phi = \mathscr{F}_2\phi$.

为了得到结论, 因而只要证明成立 $\mathscr{F}\circ\mathscr{F} = s$ 即可, 其中 $s : L^2(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ 是 $\mathscr{L}^2(\mathbf{R}^m)$ 上由 $s(\phi)(x) = \phi(-x)$ 定义的映射诱导的映射. 事实上, 这同时证明了满性与 $\overline{\mathscr{F}}$ 为 $\mathscr{F}$ 的逆. 由映射 $\mathscr{F}\circ\mathscr{F}$ 和 s 的连续性, 因此只需证明它们在 $\mathrm{Esc}(\mathbf{R}^m)$ 上相等即可, 而它是个稠密的子空间, 并且由线性性, 也只需对 $\mathrm{Esc}(\mathbf{R}^m)$ 的一个生成元族证明就可以了, 譬如对 $r \in \mathbf{N}$ 和 $\boldsymbol{k} \in \mathbf{Z}^m$ 的 $e_{r,\boldsymbol{k}}$ 构成的族. 最后, 由于这些 $e_{r,\boldsymbol{k}}$ 由函数 $\beta_m(t) = \prod_{j=1}^m \mathbf{1}_{[-\frac{1}{2},\frac{1}{2}[}(t_j)$ 出发, 通过平移和伸缩得到, 故只要证明在 $L^2(\mathbf{R}^m)$ 中成立 $\mathscr{F}(\mathscr{F}\beta_m)(t) = \beta_m(-t)$ 即可. 然而我们有 $(\mathscr{F}\beta_m)(x) = \prod_{j=1}^m \frac{\sin \pi x_j}{\pi x_j}$, 从而化为计算 $\prod_{j=1}^m \frac{\sin \pi x_j}{\pi x_j}$ 的傅里叶变换. 对于任意 m 时的论证与对于 $m=1$ 的情形相同, 故我们只证明 $m=1$ 的情形, 好处是可以使表达式短一些.

我们因而必须计算 $\alpha(t) = \frac{\sin \pi t}{\pi t}$ 的傅里叶变换. 由于 α 不是可和的, 我们不能利用表达式 $\hat{\alpha}(x) = \int_{\mathbf{R}} e^{-2i\pi xt}\alpha(t)dt$ 来进行计算. 为处理这个问题, 我们注意到 $\alpha_\lambda(t) = e^{-\pi\lambda|t|}\alpha(t)$ 当 λ 趋向 0 时, 在 $L^2(\mathbf{R}^m)$ 中趋向 α: 因为 $|\alpha_\lambda|$ 对于 $\lambda \geqslant 0$ 被强函数 $|\alpha|$ 控制, 而后者是平方可和的, 从而当 λ 趋向 0 时,$\alpha_\lambda(t)$ 对所有 $t \in \mathbf{R}$ 趋向 $\alpha(t)$. 由 $\mathscr{F}$ 的连续性得到在 $L^2(\mathbf{R}^m)$ 中,$\mathscr{F}\alpha_\lambda$ 当 λ 趋向 0 时趋向 $\mathscr{F}\alpha$. 但我们已 [350] 经计算过了 $\mathscr{F}\alpha_\lambda$(参看 IV.4.1). 并且在此公式上可清楚看到, 当 λ 趋向 0 时, 对于 $x \neq \pm\frac{1}{2}$, $\mathscr{F}\alpha_\lambda$ 趋向 $\mathbf{1}_{[-\frac{1}{2},\frac{1}{2}[}(x)$. 由此便得到, 几乎处处成立 $\mathscr{F}\alpha = \mathbf{1}_{[-\frac{1}{2},\frac{1}{2}[}$. 证完. □

注记 IV.4.4. — 在证明过程中我们已经遇到了对于平方可和而非可和的函数 ϕ 的傅里叶变换的计算问题. 它由对 ϕ 乘以 $e^{-\pi\lambda(|t_1|+\cdots+|t_m|)}$, 并让 λ 趋向 0 取极限的方法解决. 另一种解决的方法是根据控制收敛定理, 取一个其并为 $\mathbf{R}^m$ 的递增的集合的序列 $(X_N)_{N\in\mathbf{N}}$, 并将 $\mathscr{F}\phi$ 写成 $\mathscr{F}(\mathbf{1}_{X_N}\phi)$ 当 N 趋向 $+\infty$ 时的极限 (事实上, $\mathbf{1}_{X_N}\phi$ 在 $L^2(\mathbf{R}^m)$ 中趋向 ϕ, 而由于 $\mathbf{1}_{X_N}\phi$ 是平方可和的并具有界的支集, 故是可和的).

推论 IV.4.5. — 如果 $f, g \in L^2(\mathbf{R}^m)$, 则 $\int_{\mathbf{R}^m} g\hat{f} = \int_{\mathbf{R}^m} f\hat{g}$.

证明 令 $\phi_1 = \overline{\mathscr{F}}\hat{f}$, $\phi_2 = g$. 于是有 $\mathscr{F}\phi_1 = \bar{f}$, 因此

$$\int_{\mathbf{R}^m} g\hat{f} = \langle \phi_1, \phi_2 \rangle = \langle \mathscr{F}\phi_1, \mathscr{F}\phi_2 \rangle = \int_{\mathbf{R}^m} f\hat{g}.$$

这即为所证. □

3. L^1 与 L^2 中的傅里叶变换的比较

命题 IV.4.6. — 如果 $f_1 \in L^1(\mathbf{R}^m)$ 而 $f_2 \in L^2(\mathbf{R}^m)$ 有同一个傅里叶变换, 则 $f_1 = f_2$.

证明 如果 $\phi \in \mathscr{C}_c^\infty(\mathbf{R}^m)$, 则根据推论 IV.3.23, $\overline{\mathscr{F}}\phi \in L^1(\mathbf{R}^m) \cap L^2(\mathbf{R}^m)$; 特别地, $\mathscr{F}(\overline{\mathscr{F}}\phi) = \phi$. 由于 f_1, f_2 具有相同的傅里叶变换, 那么由命题 IV.3.24 和推论 IV.4.5, 并让其中的 $g = \overline{\mathscr{F}}\phi$, 便得到 $\int_{\mathbf{R}^m} f_1\phi = \int_{\mathbf{R}^m} f_2\phi$. 再由习题 III.3.13 知这表明 $f_1 = f_2$. □

命题 IV.4.7. — (在 L^1 中的傅里叶反演公式) *如果 $\phi \in L^1(\mathbf{R}^m)$ 具有一个可和的傅里叶变换, 则 $\phi = \overline{\mathscr{F}}\hat{\phi}$.*

证明 由假设有 $\hat{\phi} \in L^1(\mathbf{R}^m)$. 另外, 由于 $\phi \in L^1(\mathbf{R}^m)$, 知 $\hat{\phi}$ 有界. 因此 $|\hat{\phi}|^2 \leqslant \|\hat{\phi}\|_\infty \cdot |\hat{\phi}|$, 从而 $\hat{\phi} \in L^2(\mathbf{R}^m)$, 这使得 $\overline{\mathscr{F}}\hat{\phi}$ 成为 $L^2(\mathbf{R}^m)$ 中的一个元, 并具有与 ϕ 相同的傅里叶变换 (在 $L^2(\mathbf{R}^m)$ 中的傅里叶反演公式). 由命题 IV.4.6 便得结论. □

4. 导数

定理 IV.4.8. — (i) *如果 $f \in H^k(\mathbf{R}^m)$, 则 $(1+\|x\|^2)^{k/2}\hat{f}(x)$ 平方可和, 且如果 $\boldsymbol{\ell} \in \mathbf{N}^m$ 满足 $|\boldsymbol{\ell}| \leqslant k$, 则 $\mathscr{F}(\partial^{\boldsymbol{\ell}} f) = (2i\pi x)^{\boldsymbol{\ell}}\hat{f}$ 和 $\|(1+\|x\|^2)^{k/2}\hat{f}\|_2 \leqslant (1+\frac{m}{2\pi})^k\|f\|_{H^k}$.*

(ii) 反之, 如果 $(1+\|t\|^2)^{k/2}f(t)$ 平方可和, 则 $\hat{f} \in H^k(\mathbf{R}^m)$, 并且, 如果 $|\boldsymbol{\ell}| \leqslant k$, 则 $\partial^{\boldsymbol{\ell}}\hat{f}(x) = (-2i\pi x)^{|\boldsymbol{\ell}|}\mathscr{F}(t^{\boldsymbol{\ell}} f)$, 以及 $\|\hat{f}\|_{H^k} \leqslant (2\pi)^k\|(1+\|t\|^2)^{k/2}f\|_2$.

[351] **注记 IV.4.9.** — (i) 其中的 (i) 可特别地用于一个 $\mathscr{C}^k$ 类的, 其阶数 $\leqslant k$ 的各阶偏导数都是平方可和的函数.

(ii) 由此定理可得到索伯列夫空间 $H^k(\mathbf{R}^m)$ 的一个 "傅里叶" 的定义. 这是使得 $(1+\|x\|^2)^{k/2}\hat{f} \in L^2(\mathbf{R}^m)$ 的函数 $f \in L^2(\mathbf{R}^m)$ 的集合. 我们可以将此定义的 k 扩张到 $s \in \mathbf{R}_+$, 从而谈及对于 $s \in \mathbf{R}_+$ 的索伯列夫空间 $H^s(\mathbf{R}^m)$(甚至在略去条件 $f \in L^2(\mathbf{R}^m)$ 时可让 $s \in \mathbf{R}$, 然而那样我们就进入了广义函数空间的理论里了).

证明 我们已知, 当 $f \in \mathscr{C}_c^k(\mathbf{R}^m)$ 时有 $\mathscr{F}(\partial^{\boldsymbol{\ell}} f) = (2i\pi x)^{\boldsymbol{\ell}}\hat{f}$. 现在, $\mathscr{F}\circ\partial^{\boldsymbol{\ell}} : H^k(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ 连续: 根据 §II.2 的 5 小节知 $\partial^{\boldsymbol{\ell}} : H^k(\mathbf{R}^m) \to H^{k-|\boldsymbol{\ell}|}(\mathbf{R}^m)$ 为连续, 而包含关系 $H^{k-|\boldsymbol{\ell}|}(\mathbf{R}^m) \subset L^2(\mathbf{R}^m)$ 满足 1 – 利普希茨条件而 $\mathscr{F} : L^2(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ 是一个等距映射, 故它们的复合连续. 由于由构造知 $\mathscr{C}_c^k(\mathbf{R}^m)$ 在 $H^k(\mathbf{R}^m)$ 中稠密, 这让我们由此得到, 对于任意的 $f \in H^k(\mathbf{R}^m)$ 有 $\mathscr{F}(\partial^{\boldsymbol{\ell}} f) = (2i\pi x)^{\boldsymbol{\ell}}\hat{f}$. 利用 $\mathscr{F} : L^2(\mathbf{R}^m) \to L^2(\mathbf{R}^m)$ 是一个等距映射的事实, 我们也得到 (展开 $(1+\sum_{j=1}^m |x_j|)^k$ 为形式 $\sum_{|\boldsymbol{\ell}|\leqslant k} a_{\boldsymbol{\ell}}|x|^{\boldsymbol{\ell}}$),

$$\|(1+\|x\|^2)^{k/2}\hat{f}\|_2 \leqslant \|1+\sum_{j=1}^m |x_j|)^k\hat{f}\|_2 \leqslant \sum_{|\boldsymbol{\ell}|\leqslant k} a_{\boldsymbol{\ell}}\|x^{\boldsymbol{\ell}}\hat{f}\|_2 = \sum_{|\boldsymbol{\ell}|\leqslant k} a_{\boldsymbol{\ell}}(2\pi)^{-|\boldsymbol{\ell}|}\|\partial^{\boldsymbol{\ell}} f\|_2.$$

将每一个 $\|\partial^{\boldsymbol{\ell}} f\|_2$ 用强函数 $\|f\|_{H^k}$ 控制, 并注意到 $\sum_{|\boldsymbol{\ell}|\leqslant k} a_{\boldsymbol{\ell}}(2\pi)^{-\boldsymbol{\ell}} = (1+\frac{m}{2\pi})^k$, 便证明了 (i).

转而证明 (ii). 设 E 是那些使得 $(1+\|t\|^2)^{k/2}f$ 为平方可和的 f 的集合. 赋予 E 一个范数 $\|\ \|_E$ 为 $\|f\|_E = \|(1+\|t\|^2)^{k/2}f\|_2$. 由定义知, 映射 $f \mapsto (1+\|t\|^2)^{k/2}f$ 诱

导了从 E 到 $L^2(\mathbf{R}^m)$ 的一个等距映射, 这使 E 成了一个希尔伯特空间.

现在, 如果 f 形如 $(1+\|t\|^2)^{-k/2}g$, 其中 g 是一个阶梯函数, 则 $(1+\|t\|^2)^{k/2}f$ 可和, 于是由定理 IV.2.8 得到 $\hat{f}$ 属于 $\mathscr{C}^k$ 类, 且 $\partial^{\boldsymbol{\ell}}\hat{f}=(-2i\pi)^{|\boldsymbol{\ell}|}\mathscr{F}(t^{\boldsymbol{\ell}}f)$, 其中 $|\boldsymbol{\ell}|\leqslant k$. 由于 $\mathscr{F}:L^2(\mathbf{R}^m)\to L^2(\mathbf{R}^m)$ 是一个等距映射, 利用它则得到

$$\|\hat{f}\|_{H^k}=\sup_{|\boldsymbol{\ell}|\leqslant k}\|\partial^{\boldsymbol{\ell}}\hat{f}\|_2=\sup_{|\boldsymbol{\ell}|\leqslant k}(2\pi)^{|\boldsymbol{\ell}|}\|t^{\boldsymbol{\ell}}f\|_2\leqslant(2\pi)^k\|(1+\|t\|^2)^{k/2}f\|_2=(2\pi)^k\|f\|_E.$$

换而言之, $f\mapsto\hat{f}$ 是从具有范数 $\|\ \|_E$ 的 $(1+\|t\|^2)^{-k/2}\mathrm{Esc}(\mathbf{R}^m)$ 到具有范数 $\|\ \|_{H^k}$ 的空间 $H^k(\mathbf{R}^m)$ 的一个满足 $(2\pi)^k$ – 利普希茨条件的映射. 由于 $\mathrm{Esc}(\mathbf{R}^m)$ 在 $L^2(\mathbf{R}^m)$ 中稠密, 故空间 $(1+\|t\|^2)^{-k/2}\mathrm{Esc}(\mathbf{R}^m)$ 在 E 中稠密, 又由于 $H^k(\mathbf{R}^m)$ 紧, 故推出 $f\mapsto\hat{f}$ 诱导了一个从 E 到 H^k 的一个满足 $(2\pi)^k$ – 利普希茨条件的映射. 换句话说, 如果 $(1+\|t\|^2)^{k/2}f$ 为平方可和的, 则 $\hat{f}\in H^k(\mathbf{R}^m)$, 且 $\|\hat{f}\|_{H^k}\leqslant(2\pi)^k\|(1+\|t\|^2)^{k/2}f\|_2$.

还需证明, 在知道 $\partial^{\boldsymbol{\ell}}\hat{f}=(-2i\pi)^{|\boldsymbol{\ell}|}\mathscr{F}(t^{\boldsymbol{\ell}}f)$ 对 f 在 E 的一个稠密的子空间成立时也对于任意的 $f\in E$ 成立. 然而 $\partial^{\boldsymbol{\ell}}\circ\mathscr{F}:E\to L^2(\mathbf{R}^m)$ 连续: 因为我们刚刚才证明 [352] 了 $\mathscr{F}:E\to H^k(\mathbf{R}^m)$ 的连续性和 $\partial^{\boldsymbol{\ell}}:H^k(\mathbf{R}^m)\to H^{k-|\boldsymbol{\ell}|}(\mathbf{R}^m)\subset L^2(\mathbf{R}^m)$ 的连续性. 同样地, $f\mapsto t^{\boldsymbol{\ell}}f$ 是从 E 到 $L^2(\mathbf{R}^m)$ 的连续映射 (甚至满足 1 – 利普希茨条件), 因此 $f\mapsto(-2i\pi)^{|\boldsymbol{\ell}|}\mathscr{F}(t^{\boldsymbol{\ell}}f)$ 是从 E 到 $L^2(\mathbf{R}^m)$ 的连续映射. 有了两个在一个稠子集上重合的连续映射, 故它们相等. 证完. □



V. 全纯函数

在一个开集 Ω 上的全纯函数是一个从 Ω 到 $\mathbf{C}$ 的函数, 它属于在复意义下的 $\mathscr{C}^\infty$ 类并且是在每一点附近的它的泰勒级数的和. 这些函数有一些性质具有绝对显著的刚性, 如果参照我们所知道的单实变函数的性质似乎有些神秘. 我们遇到的最初引起惊讶的性质之一是: 一个函数为全纯的当且仅当它属于 $\mathscr{C}^1$ 类 (复意义下的)! 这是柯西积分公式 (定理 V.4.6) 的众多推论之一. 这个公式及其直接推论 (注记 V.4.9, 定理 V. 5.1, V.5.4 和 V.5.7) 连同极大模原理 (定理 V.3.11), 孤立零点定理 (定理 V.3.3) 以及下一章的柯西留数公式, 让人们能够去解决一些十分重大的问题. 可以提到其中的代数基本定理 (习题 V.3.13, 推论 V.4.15 或者习题 VI.3.21), 拉格朗日的四平方定理 (习题 VII.6.9), 四次互反律 (习题 VI.3.28), $\zeta(3)$ 的无理性 (问题 H.12), 再或者将在附录 A 中讲述的素数定理, 等等.

V.1. 全纯函数和复解析函数

1. 整级数

如果 K 是一个域, 系数在 K 中的一个整级数 (或者形式级数)[43]是指一个形如 $\sum_{n=0}^{+\infty} a_n T^n$ 的表达式, 其中的 a_n 是 K 中的元. 系数在 K 中的整级数的集合 $K[[T]]$ 包含了系数在 K 中的多项式环 $K[T]$; 我们赋予 $K[[T]]$ 一个环结构, 它是 $K[T]$ 的环结构的推广, 定义为

$$(\sum_{n=0}^{+\infty} a_n T^n) + (\sum_{n=0}^{+\infty} b_n T^n) = \sum_{n=0}^{+\infty} (a_n + b_n) T^n,$$

[43]本书采用了 "整级数 (série entièe)" 的称呼, 而非我们习惯的 "形式幂级数". 应不会与 "整函数" 混淆.

$$(\sum_{n=0}^{+\infty} a_n T^n)(\sum_{n=0}^{+\infty} b_n T^n) = \sum_{n=0}^{+\infty} (\sum_{k=0}^{n} a_k b_{n-k}) T^n.$$

定义 $F = \sum_{n\in\mathbf{N}} a_n T^n$ 的赋值 $v_T(F)$ 为: 当 $F \neq 0$ 时是使得 $a_n \neq 0$ 的 $n \in \mathbf{N}$ 的最小的 n, 而对 $F = 0$ 则定义为 $+\infty$. 我们有 $v_T(FG) = v_T(F) + v_T(G)$ 和 $v_T(F+G) \geqslant \inf(v_T(F), v_T(G))$. 定义 $|\ |_T$ 为 $|F|_T = e^{-v_T(F)}$, 则前面就等于 $|FG|_T = |F|_T |G|_T$ 和 [354] $|F+G|_T \leqslant \sup(|F|_T, |G|_T)$. 后面的这个不等式 (超度量) 比三角不等式强, 它证明了 $d(F,G) = |F-G|_T$ 是 $K[[T]]$ 上的一个距离. 容易证明 $K[[T]]$ 在此距离下是完备的, 而一个级数 $\sum_{n\in\mathbf{N}} F_n$ 收敛当且仅当 $|F_n|_T \to 0$ (等价于 $v_T(F_n) \to +\infty$), 以及 $K[T]$ 在 $K[[T]]$ 中稠密, 这证明了 $K[[T]]$ 是 $K[T]$ 在赋值 v_T (的相伴距离) 下的完备化. 这便给出了 $K[[T]]$ 的由 $K[T]$ 得到的拓扑构造[(1)].

如果 $F = \sum_{n=0}^{+\infty} a_n T^n \in K[[T]]$, 而令 $F' = \sum_{n=1}^{+\infty} n a_n T^{n-1}$ 为它的导数. 归纳定义它的 k 阶导数 $F^{(k)}$ 为 $F^{(k-1)}$ 的导数, 并令 $F^{(0)} = F$, 因此 $F^{(1)} = F'$. 2 阶导数 $F^{(2)}$ 也常常记为 F''. 直接计算表明 $\frac{1}{k!}F^{(k)} = \sum_{n=0}^{+\infty} a_{n+k}\binom{n+k}{k} T^n$.

习题 V.1.1. — (i) 证明, 如果 $F, G \in K[[T]]$, 则 $(FG)' = F'G + FG'$.

(ii) 证明, 如果 $(F_n)_{n\in\mathbf{N}}$ 是 $K[[T]]$ 中的一个序列, 使得 $\sum_{n\in\mathbf{N}} F_n$ 在 $K[[T]]$ 中收敛, 且若 F 是此级数的和, 则级数 $\sum_{n\in\mathbf{N}} F'_n$ 在 $K[[T]]$ 中收敛, 其和为 $F' = \sum_{n\in\mathbf{N}} F'_n$.

(iii) 证明, 如果 $F = \sum_{n\in\mathbf{N}} a_n T^n \in K[[T]]$, 且若 $G \in TK[[T]]$, 则 $\sum_{n\in\mathbf{N}} a_n G^n$ 在 $K[[T]]$ 中收敛, 而其极限 $F \circ G$ 满足 $(F\circ G)' = (F'\circ G)G'$.

习题 V.1.2. — 设 $(u_n)_{n\in\mathbf{N}} \in \mathbf{C}^N$ 满足递归关系 $u_{n+2} - 3u_{n+1} + 2u_n = 1, \forall n \in \mathbf{N}$, 并设 $F = \sum_{n\in\mathbf{N}} u_n T^n \in \mathbf{C}[[T]]$. 计算作为 u_0 和 u_1 函数的 $(1-3T+2T^2)F(T)$. 由此推导出对于通项 u_n 的公式.

虽然我们后面只对 $K = \mathbf{C}$ 的情形感兴趣, 但随后的例题对于特征 0 的任意域都有意义.

例题 V.1.3. — • 指数级数. 如果 $\lambda \in \mathbf{C}$, 以 $\exp(\lambda T)$ 记形式级数 $\sum_{n=0}^{+\infty} \frac{\lambda^n}{n!} T^n$. 它是微分方程 $F' = \lambda F$ 的形式解, 而它的常数项等于 1, 而且有 $\exp(\lambda T)\exp(\mu T) = \exp((\lambda+\mu)T)$.

• 幂级数. 如果 $\alpha \in \mathbf{N}$, 则根据二项式公式, $(1+T)^\alpha = \sum_{n=0}^{+\infty} \binom{\alpha}{n} T^n$, 而 $\binom{\alpha}{n}$ 当 $n > \alpha$ 时为 0. 类比地, 我们对于 $\alpha \in \mathbf{C}$ 定义 $(1+T)^\alpha$ 为整级数 $\sum_{n=0}^{+\infty} \binom{\alpha}{n} T^n$. 如果 $\alpha, \beta \in \mathbf{N}$, 则有

$$\sum_{n=0}^{+\infty} \left(\sum_{k=0}^{n} \binom{\alpha}{k} \binom{\beta}{n-k} \right) T^n = (1+T)^\alpha (1+T)^\beta = (1+T)^{\alpha+\beta} = \sum_{n=0}^{+\infty} \binom{\alpha+\beta}{n} T^n,$$

[(1)] 注意, $F \in K[[T]]$ 在知道了对任意 $n \in \mathbf{N}$ 它的前 n 个系数时就被确定了, 故得到了 $K[[T]]$ 的一个代数构造. 换句话说, F 被它在 $K[T]/(T^n)$, $n \in \mathbf{N}$ 中的像 F_n 确定, 而映射 $F \mapsto (F_n)_{n\in\mathbf{N}}$ 将 $K[[T]]$ 恒等于 $K[T]/(T^n)$ 的投射极限 $\varprojlim K[T]/(T^n)$, 即序列 $(F_n)_{n\in\mathbf{N}}$ 的集合, 其中 $F_n \in K[T]/(T^n)$, 而 $F_{n+1} \in K[T]/(T^{n+1})$ 的 mod T^n 的像为 F_n, 并且 $n \in \mathbf{N}$ 任意. 请注意这与 p-adic 数构造的相似之处.

这等价于两个变量的多项式 $\binom{X+Y}{n}$ 和 $\sum_{k=0}^{n}\binom{X}{k}\binom{Y}{n-k}$ 在 $\mathbf{N}\times\mathbf{N}$ 上取相同的值. 因此它们相等, 这让我们证明了, 对于任意的 $\alpha,\beta\in\mathbf{C}$ 成立 $(1+T)^{\alpha}(1+T)^{\beta}=(1+T)^{\alpha+\beta}$. [355]

$(1+T)^{\alpha}$ 的导数为 $\sum_{n=0}^{+\infty}(n+1)\binom{\alpha}{n+1}T^{n}=\alpha(1+T)^{\alpha-1}$, 在其中用到了 $(n+1)\binom{\alpha}{n+1}=\alpha\binom{\alpha-1}{n}$.

- 对数级数定义 $\log(1+T)$ 为级数 $\sum_{n=1}^{+\infty}\frac{(-1)^{n-1}}{n}T^{n}$. 它的导数是 $\sum_{n=0}^{+\infty}(-1)^{n}T^{n}=\frac{1}{1+T}$.

习题 V.1.4. — (i) 证明, 在 $\mathbf{C}[[T]]$ 中有 $\log(\exp(\lambda T))=\lambda T$.

(ii) 证明在 $\mathbf{C}[[T]]$ 中有 $(1+T)^{\alpha}=\exp(\alpha\log(1+T))$. (可应用算子 $(1+T)\frac{d}{dT}$ 到两端.)

习题 V.1.5. — (i) 如果 $\alpha\in\mathbf{C}$, 在 $\mathbf{C}[[T]]$ 中解微分方程 $(1+T)F'=\alpha F$, 其中满足的条件是 $F(0)=1$(即 $F=1+a_1T+\dots$).

(ii) 在 $\mathbf{Q}[[T]]$ 中解微分方程 $T^2F'+TF+F=1$.

2. 整级数的收敛半径

如果 $z_0\in\mathbf{C}$ 而 $r>0$, 以 $D(z_0,r)$ 代表中心为 z_0 半径为 r 的闭圆盘 (即满足 $|z-z_0|\leqslant r$ 的 $z\in\mathbf{C}$ 的集合), 而 $D(z_0,r^-)$ 则代表了中心为 z_0 半径为 r 的开圆盘 (即满足 $|z-z_0|<r$ 的 $z\in\mathbf{C}$ 的集合).

回忆 (小词典的 15.4 小节), 如果 $F=\sum_{n=0}^{+\infty}a_nT^n\in\mathbf{C}[[T]]$, 则存在唯一的 $\rho(F)\in\overline{\mathbf{R}}_+$ 使得当 $|z|<\rho$ 时级数 $\sum_{n=0}^{+\infty}a_nz^n$ 绝对收敛, 并且当 $|z|>\rho(F)$ 时序列 a_nz^n 不是有界的 (从而该级数发散), 这时称 $\rho(F)$ 为 F 的收敛半径. 另外, 我们有 $\rho(F)^{-1}=\limsup|a_n|^{1/n}$.

如果 $z\in D(0,\rho(F)^-)$, 则以 $F(z)$ 记级数 $\sum_{n=0}^{+\infty}a_nz^n$ 的和. 我们将下面引理的证明留给读者.

引理 V.1.6. — 如果 $F,G\in\mathbf{C}[[T]]$, 则

$$\rho(F+G)\geqslant\inf(\rho(F),\rho(G))\ 和\ \rho(FG)\geqslant\inf(\rho(F),\rho(G)),$$

并且当 $|z|<\inf(\rho(F),\rho(G))$ 时有

$$(F+G)(z)=F(z)+G(z),\ (FG)(z)=F(z)G(z).$$

例题 V.1.7. — • 如果 $\lambda\in\mathbf{C}$, 则 $\rho(\exp(\lambda T))=+\infty$.

- $\rho(\log(1+T))=1$, 而当 $\alpha\notin\mathbf{N}$ 时 $\rho((1+T)^{\alpha})=1$(否则我们就有了一个收敛半径为 $+\infty$ 的多项式了). 事实上, 如果 $\alpha\in\mathbf{C}-\mathbf{N}$, 则 $|\binom{\alpha}{n+1}/\binom{\alpha}{n}|=|\frac{\alpha-n}{n+1}|\to 1$, 从而 $|\binom{\alpha}{n}|^{1/n}\to 1$(切萨罗 (Césaro) 平均法的乘法形式).

- 级数[2] $\sum_{n=0}^{+\infty}(-1)^n n!T^n$ 的收敛半径为 0.

注记 V.1.8. — 由于在 $\mathbf{C}[[T]]$ 中 $(1+T)^{\alpha}(1+T)^{\beta}=(1+T)^{\alpha+\beta}$, 又由于这三个整级数具有 $\geqslant 1$ 的收敛半径, 故 $(1+z)^{\alpha}(1+z)^{\beta}=(1+z)^{\alpha+\beta}$ 对于任意的 $z\in D(0,1^-)$ [356] 和 $\alpha,\beta\in\mathbf{C}$ 成立. 特别地, 如果 $m\in\mathbf{N}-\{0\}$, 则 $(1+z)^{1/m}$ 是 $1+z$ 的 m 次根, 其中 $z\in D(0,1^-)$ 任意.

习题 V.1.9. — 设 $\alpha\in\mathbf{R}-\mathbf{N}$[3].

(i) 用函数 Γ 表达 $\binom{\alpha}{n}$.

(ii) 由此推出存在 $C(\alpha)\in\mathbf{C}$ 使得 $\binom{\alpha}{n}\sim C(\alpha)(-1)^n n^{-1-\alpha}$. (利用斯特林公式 (习题 IV.1.5).)

命题 V.1.10. — (i) 如果 $F=\sum_{n=0}^{+\infty}a_nT^n\in\mathbf{C}[[T]]$, 则对于任意的 $k\in\mathbf{N}$ 有 $\rho(F^{(k)})\geqslant\rho(F)$, 并且, 如果 $|z_0|+|z-z_0|<\rho(F)$, 则

$$F(z)=\sum_{k=0}^{+\infty}\left(\sum_{n=0}^{+\infty}\binom{n+k}{k}a_{n+k}z_0^n\right)(z-z_0)^k=\sum_{n=0}^{+\infty}\frac{F^k(z_0)}{k!}(z-z_0)^k.$$

(ii) 如果 $|z_0|<\rho(F)$, 则 $\lim_{z\to z_0}\frac{F(z)-F(z_0)}{z-z_0}=F'(z_0)$.

证明 如果 $|z_0|+|z-z_0|<\rho(F)$, 则有

$$\begin{aligned}\sum_{k=0}^{+\infty}\left(\sum_{n=0}^{+\infty}\binom{n+k}{k}|a_{n+k}z_0^n|\right)|z-z_0|^k&=\sum_{m=0}^{+\infty}\sum_{n+k=m}\binom{m}{k}|a_m||z_0^n||z-z_0|^k\\&=\sum_{m=0}^{+\infty}|a_m|(|z_0|+|z-z_0|)^m<+\infty,\end{aligned}$$

这证明了命题中的那个二重级数绝对收敛. 固定 k, 从而得到 $F^{(k)}$ 当 $|z_0|<\rho(F)$ 时收敛, 因此 $\rho(F^{(k)})\geqslant\rho(F)$. 另外, 我们可以任意地重新安排项, 并先对 $n+k=m$ 取和, 然后再对 m 取和. 对 $n+k=m$ 的取和得到 $\sum_{n+k=m}\binom{m}{n}a_mz_0^k(z-z_0)^n=a_mz^m$, (i) 得证.

为证明 (ii), 做变量变换 $z=z_0+h$, 则 (i) 让我们可假设 $z_0=0$. 然而有

$$\left|\frac{F(h)-F(0)}{h}-F'(0)\right|=\left|h\sum_{n=2}^{+\infty}a_nh^{n-2}\right|\leqslant|h|\left(\sum_{n=2}^{+\infty}|a_n|(\rho(F)/2)^{n-2}\right),$$

其中 $|h|<\rho(F)/2$, 又由于 $\sum_{n=2}^{+\infty}|a_n|(\rho(F)/2)^{n-2}<+\infty$, 故得到 $\frac{F(h)-F(0)}{h}-F'(0)$ 当 $h\to 0$ 时趋向 0. 证完. □

[2] 这是函数 $f(x)=\int_0^{+\infty}\frac{e^{-t}}{1+tx}dt$ 在 0 的泰勒展开式, 它在 $\mathbf{R}_+$ 上属于 $\mathscr{C}^{+\infty}$, 这告诉了欧拉 $\sum_{n=0}^{+\infty}(-1)^n n!=\int_0^{+\infty}\frac{e^{-t}}{1+x}dt$. 注意, f 甚至满足习题 V.1.5 中的微分方程 $x^2f'+xf+f=1$.

[3] 一旦我们在复平面上有了函数 Γ, 则此习题的结果可以推广到 $\alpha\in\mathbf{C}-\mathbf{N}$ 上 (参看定理 VII.2.1 和命题 VII.2.9).

注记 V.1.11. — 我们可以重新叙述此命题的 (ii) 为: 如果 $F \in \mathbf{C}[[T]]$ 具有非零的收敛半径, 则 F 在 $D(0, \rho(F)^-)$ 中是复意义下可导的, 并在复意义下 F 的导数为 F'. 总之, 可直接证明 F 在 $D(0, \rho(F)^-)$ 中属于复意义下的 $\mathscr{C}^\infty$ 类, 而且 F 的 k 阶复导数 [357] 是相伴于整级数 $F^{(k)}$ 的函数.

V.2. 全纯函数的例子

1. 定义

设 Ω 是 $\mathbf{C}$ 的一个开集, $f : \Omega \to \mathbf{C}$. 如果 $z_0 \in \Omega$ 而 $r > 0$, $D(z_0, r^-) \subset \Omega$, 称 f 在 $D(z_0, r^-)$ 上可展开为整级数是说, 如果存在收敛半径 $\geqslant r$ 的 $F \in \mathbf{C}[[T]]$, 使得对于每个 $z \in D(z_0, r^-)$ 有 $f(z) = F(z - z_0)$. 由命题 V.1.10 的 (i) 知, 如果 f 在 $D(z_0, r^-)$ 上可展开为整级数, 且若 $D(z_1, r_1^-) \subset D(z_0, r^-)$, 则 f 在 $D(z_1, r_1-)$ 上可展开为整级数.

称 f 在 z_0 附近可展开为整级数是说, 如果存在 $r > 0$ 使得 f 在 $D(z_0, r^-)$ 上可展开为整级数, 而称 f 在 Ω 上为解析的或者也称 f 在 Ω 上为全纯的是说, f 在 Ω 的每个点附近都可展开为整级数. 由注记 V.1.11 知, 一个 Ω 上的解析函数在 Ω 上属于复意义下的 $\mathscr{C}^\infty$ 类.

例题 V.2.1. — (i) 一个多项式是在 $\mathbf{C}$ 上的全纯函数.

(ii) $z \mapsto \exp(\lambda z), \lambda \in \mathbf{C}$ 在 $\mathbf{C}$ 上全纯; 它的导数为 $z \mapsto \lambda \exp(\lambda z)$.

(iii) $z \mapsto \frac{1}{z}$ 在 $\mathbf{C} - \{0\}$ 上全纯, 其导数为 $z \mapsto -\frac{1}{z^2}$.

(iv) 例题 V.1.3 中用形式级数定义的 $z \mapsto \log(1+z)$ 和 $z \mapsto (1+z)^s, s \in \mathbf{C}$ 在 $D(0, 1^-)$ 中全纯; 它们的导数分别为 $z \mapsto \frac{1}{1+z}$ 和 $z \mapsto s(1+z)^{s-1}$.

(v) 如果 f, g 在 Ω 上全纯, 则 $f + g, fg$ 在 Ω 上也都全纯, 它们的导数分别为 $f' + g'$ 和 $f'g + fg'$.

(vi) 如果 $f : \Omega_1 \to \Omega_2$ 和 $g : \Omega_2 \to \mathbf{C}$ 都为全纯的, 则 $g \circ f$ 在 Ω_1 上全纯, 其导数为 $(g' \circ f)f'$.

(vii) 如果 $f : \Omega_1 \to \Omega_2$ 为全纯的双射, 则其逆 $f^{-1} : \Omega_2 \to \Omega_1$ 也全纯.

(viii) 一个有理函数在它的极点集的开补集上全纯.

证明 (i) 显然. (ii) 和 (iv) 由例题 V.1.7 得到. 注意到当 $|z - z_0| < |z_0|$ 时有 $\frac{1}{z} = \sum_{n=0}^{+\infty} \frac{(z_0 - z)^n}{z_0^{n+1}}$ 则 (iii) 得证. (v) 来自引理 V.1.6. (vi) 和 (vii) 可直接证明, 但等到我们了解了更多知识后将给出一个漂亮的证明 (参看推论 V.4.8). 最后,(viii) 由 (i), (iii),(v) 和 (vi) 得到. □

习题 V.2.2. — (i) 证明 $z \mapsto \sin z = \frac{1}{2i}(e^{iz} - e^{-iz})$ 和 $z \mapsto \cos z = \frac{1}{2}(e^{iz} + e^{-iz})$ 在 $\mathbf{C}$ 上全纯, 而 $z \mapsto \cot \pi z = \frac{\cos \pi z}{\sin \pi z}$ 在 $\mathbf{C} - \mathbf{Z}$ 上全纯.

(ii) 证明 $z \mapsto |z|^2$ 属于 $\mathscr{C}^\infty$, 这是指在 $\mathbf{C} \cong \mathbf{R}^2$ 的实的意义下的.

[358] 2. 对数和幂函数

如果 $\alpha \in \mathbf{R}$, 则映射 $z \mapsto e^z$ 全纯并且是从带状区域 $\{z, \alpha < \mathrm{Im}(z) < \alpha + 2\pi\}$ 到去掉一条变量 α(或者 $\alpha + 2\pi$, 结果一样) 的半直线 $\mathbf{R}_+ e^{i\alpha}$ 的 $\mathbf{C}$ 上的一个双射. 此双射的逆为

$$\log_\alpha : \mathbf{C} - \mathbf{R}_+ e^{i\alpha} \to \{z, \alpha < \mathrm{Im}(z) < \alpha + 2\pi\},$$

根据例题 V.2.1(vii) 知其为全纯的.

由于在 $\mathbf{C} - \mathbf{R}_+ e^{i\alpha}$ 上 $\exp(\log_\alpha(z)) = z$, 对此关系求导则得到 $\log_\alpha$ 在 $\mathbf{C} - \mathbf{R}_+ e^{i\alpha}$ 上的导数是 $\frac{1}{z}$, 因此 $\log_\alpha$ 满足了一个对数函数应当被期待的那些性质. 唯一的问题是, 由于沿着半直线 $\mathbf{R}_+ e^{i\alpha}$ 的不连续性 (沿此半直线的"左"和"右"极限相差 $2i\pi$), 我们不能在整个 $\mathbf{C}^*$ 上定义这个对数为一个全纯函数. 问题在于事物本身的特性 [4]: 对数是一个 $\mathbf{C}^*$ 上的多值全纯函数, 上面的这些函数 $\log_\alpha$ 中的每一个都对应于一个对数分支的选取, 并在尽可能大的一个开集上全纯. 对数主分支是指函数 $\log_{-\pi}$; 因此它是定义在 $\mathbf{C}$ 去掉了负的实半直线 $\mathbf{R}_-$ 上的对数分支, 并在 1 取 0 值; 它的值的虚部在区间 $]-\pi, \pi[$ 中. 在实际应用中不会将 α 放作下标, 它要求留意在所考虑的情形中 $\log z$ 确切的意义: $\log z$ 的所有可能的值是 $2i\pi k + \log_{-\pi} z$, 其中 $k \in \mathbf{Z}$ 任意.

习题 V.2.3. — 设 log 是对数主分支.

(i) 证明 $\log z = \log |z| + i \arg z$, 其中 $\arg z \in]-\pi, \pi[$ 是 z 的主辐角.

(ii) 设 $z_1, z_2 \in \mathbf{C} - \mathbf{R}_-$, 使得 $z_1 z_2 \in \mathbf{C} - \mathbf{R}_-$. 按照各种情形确定 $\log(z_1 z_2) - \log z_1 - \log z_2$ 的值.

习题 V.2.4. — 设 $A < B$ 是两个实数, 而 $a = e^A, b = e^B$. 以 $\Omega(A, B)$ 记水平的带状区域 $\{z \in \mathbf{C}, A < \mathrm{Im}(z) < B\}$, 而以 $C(a, b)$ 记圆环 $\{z \in \mathbf{C}, a < |z| < b\}$. 设 $f : \Omega(A, B) \to \mathbf{C}$ 是周期为 1 的周期函数.

(i) 证明存在唯一的 $\tilde{f} : C(a, b) \to \mathbf{C}$ 使得对所有的 $z \in \Omega(A, B)$ 有 $f(z) = \tilde{f}(e^{2i\pi z})$.

(ii) 证明 $\tilde{f}$ 在 $C(a, b)$ 为全纯的当且仅当 f 在 $\Omega(A, B)$ 为全纯的.

如果 $s \in \mathbf{C}^*$, 以公式 $z^s = \exp(s \log z)$ 定义函数 z^s. 由于函数 $\log z$ 是多值的, 故 z^s 也如此, 因此应该像在 $\log z$ 时那样要进行一个选择. 如果 a 是 z^s 的一个可能的值, 那么其他的值便是 $e^{2i\pi k s} a$, 其中 $k \in \mathbf{Z}$. 特别地, 我们可小心地选取 $\log z$ 的一个适当分支来进行调整, 使得 z^s 在 $\mathbf{C} - \mathbf{R}_+ e^{i\alpha}$ 上全纯, 但, 如果 $s \notin \mathbf{Z}$, 则函数 z^s 不能延拓为

[4] 它大大地困扰了我们的前辈们. 伯努利和莱布尼茨 (以书信形式) 在 1712—1713 年曾对 $\log(-1)$ 的值进行过计算, $\log(-1) = 0$ 的一个理由是 $2\log(-1) = \log(-1)^2 = \log 1 = 0$, 另一个是说 $\log(-1)$ 是虚幻的, 因为 $\log(-1) = -2 - \frac{2^2}{2} - \frac{2^3}{3} - \cdots$ 不收敛 …… 直到 1749 年欧拉解释说一个复数有无穷多个对数. 读者可在习题校正 H.1.11,H.1.13 和在定理 VII.3.7 的证明中找到利用复对数的例子.

$\mathbf{C}^*$ 上的一个全纯函数. 即便我们采用了对数主分支, 也不是总能成立 $z_1^s z_2^s = (z_1 z_2)^s$. [359] 另一方面, 函数 $s \mapsto z^s$ 却在整个 $\mathbf{C}$ 上是全纯的, 并有 $z^{s_1+s_2} = z^{s_1} z^{s_2}$(如果我们无意于改变 $\log z$ 的值). 特别地, 如果 $m \in \mathbf{N} - \{0\}$, 则不管对数分支如何选取, $z^{1/m}$ 总是 z 的 m 次根.

注记 V.2.5. — 我们将在后面 (命题 V.4.10 和习题 V.4.12) 看到, 如果选取了对数主分支, 则 $z \mapsto \log(1+z)$ 和 $z \mapsto (1+z)^s$, $s \in \mathbf{C}$ 在其上的限制与例题 V.2.1 的 (iv) 中函数相同.

习题 V.2.6. — (i) 设 $\Omega = \mathbf{C} - [0,1]$. 证明存在两个函数 f, 它们在 Ω 上全纯而其平方都为 $z \mapsto z(z-1)$.

(ii) 设 $a_1, \ldots, a_{2n}$ 是 $\mathbf{C}$ 的不同的元. 证明, 存在 $1, \ldots, 2n$ 的一个置换 σ 使得线段 $[a_{\sigma(2i-1)}, a_{\sigma(2i)}]$, $1 \leqslant i \leqslant n$ 互不相交, 并且如果 Ω 是这些线段的补开集, 则存在 Ω 上的两个全纯函数 f, 其平方都为 $z \mapsto \prod_{i=1}^{2n}(z-a_i)$.

V.3. 全纯函数的基本性质

1. 柯西–黎曼关系

注记 V.3.1. — (i) 我们也可将全纯函数 f 想成是变量 $x = \mathrm{Re}(z)$, $y = \mathrm{Im}(z)$ 的取复数值的函数. 以 P 和 Q 记 f 的实部和虚部, 这让我们将 f 看作为从 $\mathbf{R}^2$ 中的一个开集到 $\mathbf{R}^2$ 的一个 $\mathscr{C}^1$ 类 (甚至是 $\mathscr{C}^\infty$ 类) 的函数. 在复意义下 f 在 z_0 的可导性于是可以这样表达, 即 f 在 z_0 的微分是一个相似变换, 它由 f 的实部和虚部在 z_0 的偏导数之间的柯西–黎曼关系表达:

$$\frac{\partial P}{\partial x}(z_0) = \frac{\partial Q}{\partial y}(z_0) = \mathrm{Re}(f'(z_0)) \quad \text{和} \quad \frac{\partial P}{\partial y}(z_0) = -\frac{\partial Q}{\partial x}(z_0) = -\mathrm{Im}(f'(z_0)).$$

f 在 z_0 的雅可比因此为 $|f'(z_0)|^2$; 特别地, 它为 0 等价于 $f'(z_0) = 0$.

(ii) 由于这些相似变换具有保持向量角 (而不是长度) 不变的性质, 因此一个全纯函数 f 继承了这个性质, 从而是保角的, 譬如, 这表明, 如果 $f'(z_0) \neq 0$, 则它将在 z_0 交成直角的两条曲线变换为在 $f(z_0)$ 交于直角的两条曲线.

(iii) 反之, 设 $f : \Omega \to \mathbf{C}$ 是一个 $\mathscr{C}^1$ 类的 x, y 的函数. 设 $\frac{\partial}{\partial z}$ 和 $\frac{\partial}{\partial \bar{z}}$ 为由

$$\frac{\partial}{\partial z} = \frac{1}{2}(\frac{\partial}{\partial x} - i\frac{\partial}{\partial y}) \quad \text{和} \quad \frac{\partial}{\partial \bar{z}} = \frac{1}{2}(\frac{\partial}{\partial x} + \frac{\partial}{\partial y})$$

定义的微分算子. 这些记号由下面的公式说明了它们的合理性:

$$\frac{\partial}{\partial z} z = 1, \quad \frac{\partial}{\partial z} \bar{z} = 0, \quad \text{和} \quad \frac{\partial}{\partial \bar{z}} z = 0, \quad \frac{\partial}{\partial \bar{z}} \bar{z} = 1.$$

由此得到, 在 $h = 0$ 的邻域中有 $f(z_0+h) = f(z_0) + \frac{\partial f}{\partial z}(z_0) \cdot h + \frac{\partial f}{\partial \bar{z}}(z_0) \cdot \bar{h} + o(|h|)$. f [360]

的微分是一个相似变换当且仅当 $\frac{\partial f}{\partial \bar{z}}(z_0) = 0$. 因此, f 在 z_0 为复意义下可微当且仅当 $\frac{\partial f}{\partial \bar{z}}(z_0) = 0$. 这让我们看出在复意义下的 $\mathscr{C}^1$ 类函数是一个"只与 z 有关而与 $\bar{z}$ 无关"的函数 (5), 并多少解释了命题 V.4.7 的秘密.

习题 V.3.2. — (i) 设 $P \in \mathbf{C}[X]$, 且 $\deg P \geqslant 2$. 证明如果 P 在 $\mathbf{C}$ 上不取零值, 则 $1/P$ 及其对于 x 和 y 的偏导数都在 $\mathbf{C} \cong \mathbf{R}^2$ 上平方可和. 由此得出 $1/P$ 的傅里叶变换 (看作 x 和 y 的函数) 恒等于 0, 然后推出 $\mathbf{C}$ 为代数闭域.

(ii) 改变上述推理: 只利用在 $L^1(\mathbf{C})$ 中的傅里叶变换.

2. 孤立零点定理和解析延拓的唯一性

如果 f 在 Ω 上解析, 且 $z_0 \in \Omega$; 定义 f 在 z_0 的零点的阶 $v_{z_0}(f) \in \mathbf{N} \cup \{+\infty\}$ 为使得 $f = F(z - z_0)$ 的整级数 F 的赋值 $v_T(F)$. 如果这个阶为 $+\infty$, 这表明 f 在 z_0 的一个邻域中恒等于 0 (即存在 $r > 0$ 使得当 $z \in D(z_0, r^-)$ 时有 $f(z) = 0$). 如果这个阶等于 k, 为有限的, 则 F 可分解为 $F = T^k G$, 其中 $G(0) \neq 0$. 由连续性知, $G(z - z_0)$ 在 z_0 的一个邻域上不取零, 这证明了 z_0 在此邻域中为孤立零点.

定理 V.3.3. — (孤立零点) 设 Ω 是 $\mathbf{C}$ 的一个连通开集. 如果 f 是 Ω 上的一个不恒等于 0 的全纯函数, 且若 $z_0 \in \Omega$ 是 f 的一个零点, 则存在 $r > 0$ 使得 z_0 是 $D(z_0, r)$ 中的孤立零点.

证明 根据定理前的讨论, z_0 是一个非孤立零点当且仅当 $v_{z_0}(f) = +\infty$. 由于对于 $n \in \mathbf{N}$ 的闭集 $\{z, f^{(n)}(z) = 0\}$ 的交是那些非孤立零点的集合, 因而这是个闭集, 而又如果对所有 $n \in \mathbf{N}$ 有 $f^n(z_0) = 0$, 同时如果 f 在 $D(z_0, r^-)$ 中可展开为整级数, 则 f 在 $D(z_0, r^-)$ 中恒等于 0, 故非孤立零点的集合又为开集. 但由于 Ω 连通, 从而推出非孤立零点的集合为整个 Ω (在这种情形 f 恒等于零), 于是此集合为空. 得证. □

习题 V.3.4. — 设 $f : \Omega \to \mathbf{C}$ 全纯, 且 $x_0 \in \Omega$ 及 $r > 0$ 使得 $D(x_0, r) \subset \Omega$. 假设 $f(x_0) \neq 0$; 证明 f 在 $D(x_0, r)$ 中只有有限个零点.

习题 V.3.5. — 设 f 在 $\mathbf{C}$ 上全纯, 且对于所有 $n \in \mathbf{N} - \{0\}$ 满足 $f(\frac{1}{n}) = \frac{1}{n^2}$. 证明对于所有 $z \in \mathbf{C}$, $f(z) = z^2$.

[361] **习题 V.3.6.** — 能够找到这样的函数吗, 它属于 $\mathscr{C}^\infty$, 不恒等于零, 具有在 $\mathbf{R}$ 中的紧支集, 并且它的傅里叶变换也具有紧支集?

推论 V.3.7. — (解析延拓的唯一性) 设 $\Omega \subset \Omega'$ 是 $\mathbf{C}$ 的两个非空开集. 如果 Ω' 连通且 f 和 g 是 Ω' 上的两个解析函数, 并限制在 Ω 上相等, 则在整个 Ω' 上 $f = g$.

证明 将孤立零点定理用于 $f - g$ 即可. □

---

(5)不应该从字面上来理解, 因为 $\bar{z}$ 和 z 并不是无关的, 但是如果将一个 $x = \frac{1}{2}(z + \bar{z}), y = \frac{1}{2i}(z - \bar{z})$ 的多项式看作 z 和 $\bar{z}$ 的多项式, 则这是可以理解的: $P(x, y)$ 定义了一个全纯函数当且仅当多项式 $Q(z, \bar{z}) = P(\frac{1}{2}(z + \bar{z}), \frac{1}{2i}(z - \bar{z}))$ 不含有 $\bar{z}$ 的项.

注记 V.3.8. — 设 f 是 $\mathbf{C}$ 中开集 Ω 上的一个全纯函数, 且 Ω' 是 $\mathbf{C}$ 的一个包含 Ω 的连通开集. 一般地, 不能找到一个 Ω' 上的全纯函数 g 使它在 Ω 上的限制等于 f. 当这成为可能时, 上面的推论证明了 g 是唯一的; 称其为 f 到 Ω' 的解析延拓.

我们将在后面关注这个问题. 如果 Ω_1, Ω_2 是包含 Ω 的两个开集, 并在它们上分别有 f 的两个解析延拓 f_1, f_2, 这时, 一般地, 我们并不能断言在 $\Omega_1 \cap \Omega_2$ 上有 $f_1 = f_2$ (问题在于没有理由认为 $\Omega_1 \cap \Omega_2$ 是连通的). 对数给出了这种现象的一个例证. 显然, 如果 f 具有到整个 $\mathbf{C}$ 的一个解析延拓, 这个解析延拓则无疑是唯一的了.

例题 V.3.9. — 定义在 $D(0,1^-)$ 上的解析函数 $f(z) = \sum_{n=0}^{+\infty} z^n$ 有一个在 $\mathbf{C} - \{1\}$ 上的解析延拓: 事实上, 它在 $D(0,1^-)$ 上与 $\frac{1}{1-z}$ 相同[6]. 这个例子不能使人完全信服, 因为函数 $\frac{1}{z-1}$ 明显地在 $\mathbf{C} - \{1\}$ 上全纯, 但在后面我们将见到不太平凡的一些例子 (譬如, 例题 V.5.9, 定理 VII.3.4 和 VII.4.4, 或者问题 H.10).

习题 V.3.10. — 证明 $f(z) = \sum_{n=0}^{+\infty} z^{n!}$ 在 $D(0,1^-)$ 中全纯, 但没有到任何一个严格包含 $D(0,1^-)$ 的连通开集上的解析延拓[7]. 对 $\sum_{n=0}^{+\infty} \frac{z^{n!}}{n!}$ 又如何?

3. 最大值原理

[362]

定理 V.3.11. — (最大值原理) *如果 Ω 是 $\mathbf{C}$ 的一个连通开集, 且 $z_0 \in \Omega$, 又如果 f 在 Ω 上全纯, 且如果 $|f|$ 在 z_0 具有局部极大值, 则 f 在 Ω 上为常数.*

证明　如果 f 在 Ω 上不为常数. 则 $f - f(z_0)$ 在 Ω 上不恒等于 0, 而 Ω 连通, 于是 $f - f(z_0)$ 在 z_0 附近展开的整级数不恒等于 0. 故存在 $k \in \mathbf{N} - \{0\}$ 及 $\alpha \in \mathbf{C}^*$ 使得 $f(z) = f(z_0) + \alpha \cdot (z - z_0)^k + (z - z_0)^k \varepsilon_0(z)$, 其中 $\lim_{z \to z_0} \varepsilon_0(z) \to 0$.

- 如果 $f(z_0) = 0$, 则 z_0 是 f 的一个孤立零点, 且对任意的在 z_0 附近的任意点 z 有 $|f(z)| > f(z_0)|$; 特别地, 这表明 $|f|$ 在 z_0 不具有局部极大值.
- 如果 $f(z_0) \neq 0$, 令 β 为满足 $\beta^k = \alpha^{-1} f(z_0)$ 的数. 于是有 $f(z_0 + t\beta) = f(z_0)(1 + t^k + t^k \varepsilon_1(t))$, 其中 $\lim_{t \to 0} \varepsilon_1(t) = 0$. 这表明对于充分小的 $t > 0$, 有 $|f(z_0 + t\beta)| > |f(z_0)|$, 于是 $|f|$ 在 z_0 不具有局部极大值.

---

[6] 因此希望写成 $1 + 2 + 4 + 8 + \cdots \doteq -1$, 欧拉就曾毫无顾忌地这样做了. 按同一思路, 我们有 (例题 VII.3.6)

$$1+1+1+\cdots = \zeta(0) = -\frac{1}{2}, \quad 1+2+3+4+\cdots = \zeta(-1) = -\frac{1}{12}, \quad 1+4+9+16+\cdots = \zeta(-2) = 0, \ldots.$$

处理发散级数虽然有趣但却要求有一定的技巧. 例如, 不应该混淆 $\sum_{n=0}^{+\infty} 1 = 1 + \zeta(0) = \frac{1}{2}$ 与 $\sum_{n=1}^{+\infty} 1 = \zeta(0) = -\frac{1}{2}$. 物理学家们需要一些处理具体物质上的熟练技巧; 而数学家们, 自从柯西在巴黎综合理工大学所著的《分析教程》(1821 年出版) 中说了一段话后, 则要有更为复杂的思考了. 他说的是: "*我不得不承认许多主张, 它们最初看起来可能有点难于接受. 例如 (……) 一个发散级数没有和.*"

[7] 虽然相当困难但可以证明, 如果 $f = \sum_{n=0}^{+\infty} a_n z^n$, $a_n \in \mathbf{Z}$, $n \in \mathbf{N}$ 的收敛半径为 1, 并且, 如果存在一个严格包含 $D(0,1^-)$ 的连通开集, 在其上 f 具有一个解析延拓, 则 f 是个形如 $\frac{P(z)}{(1-z^N)^k}$ 的有理分式, 其中 P 是一个系数在 $\mathbf{Z}$ 中的多项式 (波利亚–卡尔松 (Pólya-Carlson) 定理 (1921)), 参看问题 H.13, 那里有此结果的原型.

断言得证. □

注记 V.3.12. — 最大值原理常常以下面的形式应用: 一个全纯函数在边界上达到其最大值. 换而言之, 如果 K 是一个紧集而 f 在包含 K 的一个开集上全纯, 则 $|f|$ 在 K 上的最大值在 K 的边界上达到.

习题 V.3.13. — 设 $P \in \mathbf{C}[X]$ 非常值. 证明如果 P 在 $\mathbf{C}$ 上不取零值, 则 $|1/P|$ 在 $\mathbf{C}$ 的某点达到最大. 由此推出 $\mathbf{C}$ 为代数闭域.

习题 V.3.14. — 设 $a < b \in \mathbf{R}$, 且 f 在竖直带状集 $B = \{z \in \mathbf{C}, a \leqslant \mathrm{Re}(z) \leqslant b\}$ 的一个开邻域中全纯. 假设 f 在直线 $\mathrm{Re}(z) = a$ 和 $\mathrm{Re}(z) = b$ 上有界.

(i) 证明, 如果存在 $C > 0$ 和 $c > 0$, 使得对于任意的 $z \in B$ 有 $|f(z)| \leqslant Ce^{c|\mathrm{Im}(z)|}$, 则 f 在 B 上有界. (考虑函数 $e^{\varepsilon z^2} f(z)$.)

(ii) 同样证明, 如果存在 $C > 0$, $c > 0$ 和 $N \in \mathbf{N}$, 使得对于任意的 $z \in B$ 有 $|f(z)| \leqslant Ce^{c|\mathrm{Im}(z)|^N}$, 则 f 在 B 上有界.

(iii) 构造一个 $\mathbf{C}$ 上的全纯函数, 使得它在每条直线 $\mathrm{Re}(z) = a$ 和 $\mathrm{Re}(z) = b$ 上有界, 而在 B 上无界.(考虑指数的指数.)

习题 V.3.15. — (施瓦茨引理) 设 $D = \{z \in \mathbf{C}, |z| < 1\}$, 且 f 是从 D 到 D 的全纯函数, 并满足 $f(0) = 0$.

(i) 证明对于任意的 $z \in D$ 有 $|f(z)| \leqslant |z|$.(考虑 $z \mapsto g(z) = \frac{f(z)}{z}$.)

(ii) 证明, 如果 $|f'(0)| = 1$, 则对任意的 $z \in D$ 有 $f(z) = f'(0)z$.

(iii) 证明, 如果 f 是 D 到 D 的一个全纯的双射, 且 $f(0) = 0$, 则存在 $\theta \in [0, \pi]$ 使得对任意的 $z \in D$ 有 $f(z) = e^{2i\theta} z$.

(iv) 证明, 如果 f 不是一个双射, 则对于 D 的任一个紧集 K, 存在 $c_K < 1$ 使得对于所有的 $z \in K$ 有 $|f(z)| \leqslant c_K |z|$.

(v) 设 $f^{\circ n} = f \circ f \circ \cdots \circ f$($n$ 次). 证明, 如果 f 不是一个双射, 则在 D 的任一个紧集上 $f^{\circ n}$ 一致地趋向 0.

习题 V.3.16. — 设 $\mathscr{H} = \{z \in \mathbf{C}, \mathrm{Im}(z) > 0\}$ 是庞加莱半平面.

(i) 证明, 如果 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{R})$, 则 $\gamma \cdot z = \frac{az+b}{cz+d} \in \mathscr{H}$, 并有 $\gamma_1\gamma_2 \cdot z = \gamma_1 \cdot (\gamma_2 \cdot z)$.

[363] (ii) 由此推出, 映射 $\gamma \mapsto \varphi_\gamma$ 是从 $\mathbf{SL}_2(\mathbf{R})$ 到 $\mathscr{H}$ 的双全纯群 $\mathrm{Aut}(\mathscr{H})$ 的一个群同态, 而其中的 φ_γ 是变换 $z \mapsto \gamma \cdot z$.

(iii) 证明, 如果 $z \in \mathscr{H}$, 则存在 $\gamma \in \mathbf{SL}_2(\mathbf{R})$ 满足 $z = \gamma \cdot i$. 由此推出, 如果 $\varphi \in \mathrm{Aut}(\mathscr{H})$, 则存在 $\gamma \in \mathbf{SL}_2(\mathbf{R})$) 使得 i 是 $\varphi_\gamma \circ \varphi$ 的不动点.

(iv) 设 $h(z) = \frac{i-z}{i+z}$. 证明 h 是一个从 $\mathscr{H}$ 到 D 的一个双全纯映射, 且其逆 h^{-1} 由公式 $h^{-1}(z) = i\frac{1-z}{1+z}$ 给出.

(v) 利用施瓦茨引理 (习题 V.3.15) 证明, 如果 $\varphi \in \mathrm{Aut}(\mathscr{H})$ 使 i 不动, 则存在 $\theta \in [0,\pi]$ 使得 $\varphi(z) = \frac{z\cos\theta+\sin\theta}{-z\sin\theta+\cos\theta}$. (考虑 $\psi = h\circ\varphi\circ h^{-1}$.)

(vi) 证明 $\gamma \mapsto \varphi_\gamma$ 诱导了一个从 $\mathbf{SL}_2(\mathbf{R})$) 到 $\mathrm{Aut}(\mathscr{H})$ 的满射; 由此推出 $\mathrm{Aut}(\mathscr{H})$ 与 $\mathbf{SL}_2(\mathbf{R})/\{\pm 1\}$ 同构.

V.4. 柯西积分公式及其推论

1. 关于道路

在 $\mathbf{C}$ 的一个开集 Ω 中的一条道路 γ (理解为分段 $\mathscr{C}^1$ 的) 是一个从 $\mathbf{R}$ 的一个紧区间 $[a,b]$ 到 Ω 的连续映射 $\gamma:[a,b]\to\Omega$, 且是分段 $\mathscr{C}^1$ 的. 点 $\gamma(a)$ 是 γ 的起点而 $\gamma(b)$ 则是其终点. 称 γ 是一条闭道是说, 如果它的起点和终点重合. 如果 $t\in[a,b]$ 是一个这样的点, 在此点 γ 的左、右导数不同, 则称 $\gamma(t)$ 为 γ 的一个角点. 由假设知, γ 只有有限个角点.

如果 $\gamma(t) = x(t)+iy(t)$, 定义 γ 的长 $\lg(\gamma)$ 为

$$\lg(\gamma) = \int_a^b \sqrt{x'(t)^2+y'(t)^2}dt = \int_a^b |\gamma'(t)|dt.$$

道路的长在再参数化下不变 (γ 的再参数化是一条形如 $\gamma_1 = \gamma\circ\varphi$ 的道路, 其中 $\varphi:[a_1,b_1]\to[a,b]$ 是一个 $\mathscr{C}^1$ 类的递增双射). 事实上, 我们有

$$\begin{aligned}\lg(\gamma_1) &= \int_{a_1}^{b_1} \sqrt{(x\circ\varphi)'(t)^2+(y\circ\varphi)(t)^2}dt\\ &= \int_{a_1}^{b_1} \sqrt{(x'\circ\varphi)(t)^2\varphi'(t)^2+(y'\circ\varphi)(t)^2\varphi'(t)^2}dt\\ &= \int_{a_1}^{b_1} \sqrt{(x'\circ\varphi)(t)^2+(y'\circ\varphi)(t)^2}\varphi'(t)dt\\ &= \int_a^b \sqrt{x'(s)^2+y'(s)^2}ds = \lg(\gamma).\end{aligned}$$

如果 $\gamma:[a,b]\to\Omega$ 是一条道路, 定义 γ 的反向道路 $\gamma^{\mathrm{opp}}:[a,b]\to\Omega$ 为 $\gamma^{\mathrm{opp}}(t) = \gamma(a+b-t)$.

如果 $\gamma_1:[a_1,b_1]\to\Omega$ 和 $\gamma_2:[a_2,b_2]\to\Omega$ 为两条道路, 称 γ_1 和 γ_2 是可连接的是说 γ_2 的起点与 γ_1 的终点重合, 并定义 $\gamma_1\cdot\gamma_2:[a_1,b_2-a_2+b_1]\to\Omega$, 它由 γ_1 与 γ_2 连接而成, 即当 $t\in[a_1,b_1]$ 时 $\gamma_1\cdot\gamma_2(t) = \gamma_1(t)$, 而当 $t\in[b_1,b_2-a_2+b_1]$ 时, $\gamma_1\cdot\gamma_2(t) = \gamma_2(t+a_2-b_1)$.

例题 V.4.1. — (一些标准的道路)

- 如果 $z_0\in\mathbf{C}$ 而 $r>0$, 则以 $C(z_0,r):[0,1]\to\mathbf{C}$ 记道路 $t\mapsto z_0+re^{2i\pi t}$; 这是中心在 z_0 的半径为 r 的沿正方向的圆. 其长为 $2\pi r$.

[364] • 如果 $a, b \in \mathbf{C}$, 以 $[a,b]:[0,1]\to\mathbf{C}$ 记道路 $t\mapsto a+t(b-a)$; 这是一个起点为 a 终点为 b 的线段. 它的长为 $|b-a|$.

2. 沿道路的积分

将 $\mathbf{C}$ 等同于 $\mathbf{R}^2$, 并将 z 写成 $x+iy$. 在 $\mathbf{C}$ 的开集 Ω 上的 1-形式是一个形如 $Pdx+Qdy$ 的表达式[8], 其中 P, Q 是 Ω 上的一个连续函数. 如果 f 是 Ω 上的一个 $\mathscr{C}^1$ 类的函数, f 的微分 df 可以看作一个 1-形式: $df=\frac{\partial f}{\partial x}dx+\frac{\partial f}{\partial y}dy$.

如果 $\omega=Pdx+Qdy$ 是 Ω 上的一个 1-形式, 且 $\gamma:[a,b]\to\Omega$ 为 Ω 中的一条道路, 定义积分 $\int_\gamma\omega$ 为

$$\begin{aligned}\int_\gamma\omega&=\int_a^b P(\gamma(t))d(x(\gamma(t)))+Q(\gamma(t))d(y(\gamma(t)))\\&=\int_a^b(P(\gamma(t))(x\circ\gamma)'(t)+Q(\gamma(t))(y\circ\gamma)'(t))dt.\end{aligned}$$

在上面的积分中, $(x\circ\gamma)'(t)$ 和 $(y\circ\gamma)'(t)$ 除了在角点外全有定义, 但由于它们只有有限个, 不影响此积分.

定理 V.4.2. — (i) $\int_\gamma\omega$ 在再参数化下不变: 如果 $\varphi:[a_1,b_1]\to[a,b]$ 是一个 $\mathscr{C}^1$ 类递增双射, 且若 $\gamma_1=\gamma\circ\varphi$, 则 $\int_{\gamma_1}\omega=\int_\gamma\omega$.

(ii) $\int_{\gamma^{\mathrm{opp}}}\omega=-\int_\gamma\omega$,

(iii) 如果 γ_1 和 γ_2 可连接, 则 $\int_{\gamma_1\cdot\gamma_2}\omega=\int_{\gamma_1}\omega+\int_{\gamma_2}\omega$,

(iv) 如果 $\omega=df$, 则 $\int_\gamma\omega=f(\gamma(b))-f(\gamma(a))$.

证明 (i) 来自以下的计算:

$$\begin{aligned}\int_{\gamma_1}\omega&=\int_{a_1}^{b_1}(P(\gamma\circ\varphi(t))(x\circ\gamma\circ\varphi)'(t)+Q(\gamma\circ\varphi(t))(y\circ\gamma\circ\varphi)'(t))dt\\&=\int_{\varphi(a_1)}^{\varphi(b_1)}(P(\gamma(s))(x\circ\gamma)'(s)+Q(\gamma(s))(y\circ\gamma)'(s))ds=\int_\gamma\omega.\end{aligned}$$

---

[8] 更一般地, 如果 ω 是 $\mathbf{R}^n$ 的开集且 $p\leqslant n$, ω 上的一个 p-形式是指形如

$$\omega=\sum_{i_1<i_2<\cdots<i_p}f_{i_1,\ldots,i_p}dx_{i_1}\wedge\cdots\wedge dx_{i_p},$$

其中这些 $f_{i_1,\ldots,i_p}$ 是 Ω 上的连续函数. (按约定, 一个 0-形式是 Ω 上的连续函数.) 我们也常常将 Ω 上的一个 p-形式看作为 Ω 上的一个取值于交错的 p-线性形式的连续函数 $x\mapsto\omega_x$: 如果 $u_1,\ldots,u_p$ 是 $\mathbf{R}^n$ 的 p 个向量, 其中 $u_i=(u_{i,1},\ldots,u_{i,n})$, 且若 $x\in\Omega$ 则 (参看小词典的习题 6.1):

$$\omega_x(u_1,\ldots,u_p)=\sum_{i_1<i_2<\cdots<i_p}f_{i_1,\ldots,i_p}(x)\sum_{\sigma\in S_p}\mathrm{sign}(\sigma)u_{1,i_{\sigma(1)}}\ldots u_{p,i_{\sigma(p)}}.$$

在微分几何中这些东西有着重要的作用. 基本的例子是 1-形式 df, 其中 f 是 Ω 上的 $\mathscr{C}^1$ 类的函数. 它在 x 的值是线性形式 $u\mapsto\lim_{t\to0}\frac{f(x+tu)-f(x)}{t}=\sum_{i=1}^n\frac{\partial f}{\partial x_i}(x)u_i$.

通过变量变换 $t \mapsto a+b-t$, 则 (ii) 由积分界限的交换得到.

(iii) 直接可得. [365]

(iv) 由以下计算得到:

$$\int_\gamma df = \int_a^b \left(\frac{\partial f}{\partial x}(\gamma(t))(x\circ\gamma)'(t) + \frac{\partial f}{\partial y}(\gamma(t))(y\circ\gamma)'(t)\right)dt$$
$$= \int_a^b (f\circ\gamma)'(t)dt = f(\gamma(b)) - f(\gamma(a)). \qquad \square$$

以 dz 代表 $dx + idy$. 如果 f 是 Ω 上的一个连续函数, 则 1-形式 $f(z)dz$ 不外乎是 $f(x+iy)dx + if(x+iy)dy$. 如果 $\gamma : [a,b] \to \Omega$ 是一条分段 $\mathscr{C}^1$ 类道路, 则

$$\int_\gamma f(z)dz = \int_a^b f(\gamma(t))((x\circ\gamma)'(t) + i(y\circ\gamma)'(t))dt = \int_a^b f(\gamma(t))\gamma'(t)dt.$$

因为 $\lg(\gamma) = \int_a^b |\gamma'(t)|dt$, 故立即可得下面非常有用的控制强函数引理.

引理 V.4.3. — $|\int_\gamma f(z)dz| \leqslant \lg(\gamma)\cdot\sup_{z\in\gamma([a,b])}|f(z)|$.

例题 V.4.4. — (标准道路上的积分)

(i) 如果 $z_0 \in \mathbf{C}$ 且 $r > 0$, 则 $\int_{C(z_0,r)} f(z)dz = 2i\pi r\int_0^1 f(z_0 + re^{2i\pi t})e^{2i\pi t}dt$.

(ii) 如果 $a, b \in \mathbf{C}$, 则 $\int_{[a,b]} f(z)dz = (b-a)\int_0^1 f(a + t(b-a))dt$.

习题 V.4.5. — 设 Ω_1, Ω_2 为 $\mathbf{C}$ 的开集, $f : \Omega_1 \to \mathbf{C}$ 连续, 而 $\varphi : \Omega_2 \to \Omega_1$ 全纯. 证明, 如果 $\gamma : [a,b] \to \Omega_2$ 是一条道路, 则 $\int_\gamma (f\circ\varphi)\varphi'(z)dz = \int_{\varphi\circ\gamma} f(z)dz$.

3. 柯西积分公式

定理 V.4.6. — (柯西积分公式, 1825) *设 f 是 $\mathbf{C}$ 中开集 Ω 上属于复意义下 $\mathscr{C}^1$ 类的函数, 且设 $z_0 \in \Omega$ 而 $r > 0$, 使得 $D(z_0, r) \subset \Omega$. 于是, 对所有 $z \in D(z_0, r^-)$ 有*

$$f(z) = \frac{1}{2i\pi}\int_{C(z_0,r)} \frac{f(w)}{w-z}dw.$$

证明 如果 $w \in C(z_0, r)$ 而 $z \in D(z_0, r^-)$, 则有 $|z - z_0| < |w - z_0|$, 因此 $\frac{1}{w-z} = \sum_{n=0}^{+\infty}\frac{(z-z_0)^n}{(w-z_0)^{n+1}}$. 由于此级数的收敛性在这个圆上是一致的, 故我们可以交换和与积分, 令 $w = z_0 + re^{2i\pi t}$, 这便给出了

$$\int_{C(z_0,r)}\frac{dw}{w-z} = \sum_{n=0}^{+\infty}\int_{C(z_0,r)}\frac{(z-z_0)^n}{(w-z_0)^{n+1}}dw = \sum_{n=0}^{+\infty}\int_0^1\frac{(z-z_0)^n}{(re^{2i\pi t})^{n+1}}2i\pi re^{2i\pi t}dt,$$

并由于该级数除了 $n = 0$ 的项外每项都为 0, 而 $n = 0$ 的项为 $2i\pi$, 于是得到 $\int_{C(z_0,r)}\frac{dw}{w-z} = 2i\pi$. 由此推出恒等式

$$\left(\frac{1}{2i\pi}\int_{C(z_0,r)}\frac{f(w)}{w-z}dw\right) - f(z) = \frac{1}{2i\pi}\int_{C(z_0,r)}\frac{f(w)-f(z)}{w-z}dw.$$

[366] 现在, $\frac{f(w)-f(z)}{w-z}=\int_0^1 f'(w+u(z-w))du$, 而

$$\int_{C(z_0,r)}\int_0^1 f'(w+u(z-w))dudw=\int_0^1\int_0^1 f'((1-u)(z_0+re^{2i\pi t})+uz)du2i\pi re^{2i\pi t}dt.$$

由于函数 $(t,u)\mapsto f'((1-u)(z_0+re^{2i\pi t})+uz)2i\pi re^{2i\pi t}$ 在紧集 $[0,1]^2$ 上连续, 故可和; 于是可以用富比尼定理来交换变量. 但, 当 $u\neq 1$ 时

$$\int_0^1 f'((1-u)(z_0+re^{2i\pi t})+uz)2i\pi re^{2i\pi t}dt=[\frac{1}{1-u}f((1-u)(z_0+re^{2i\pi t})+uz)]_{t=0}^{t=1}=0.$$

因此知此二重积分为零, 得到断言. □

4. 复可导的函数是全纯的

定理 V.4.6 有一些使得熟悉单实变函数的人深感惊讶的推论[9]. 下面的命题 V.4.7 是这方面的一个基本例子. 它证明了一个复意义下的 $\mathscr{C}^1$ 类函数实际上是全纯的 (因而自然是 $\mathscr{C}^\infty$ 的). 注记 V.4.9 和定理 V.5.1 给出了有点神秘的另外的例子.

命题 V.4.7. — *如果 f 满足柯西公式, 并且如果对于 $n\in\mathbf{N}$ 定义 $a_n\in\mathbf{C}$ 为*

$$a_n=\frac{1}{2i\pi}\int_{C(z_0,r)}\frac{f(w)}{(w-z_0)^{n+1}}dw,$$

则级数 $F(T)=\sum_{n=0}^{+\infty}a_nT^n$ 的收敛半径 $\geqslant r$, 并且对于任意的 $z\in D(z_0,r^-)$ 有 $f(z)=F(z-z_0)$.

证明 令 $M=\sup_{w\in C(z_0,r)}|f(w)|$(由于 f 在紧集 $C(z_0,r)$ 上连续故 M 为有限的). 故有

$$|a_n|\leqslant\frac{1}{2\pi}\lg(C(z_0,r))\cdot(\sup_{w\in C(z_0,r)}|\frac{f(w)}{(w-z_0)^{n+1}}|)\leqslant Mr^{-n}.$$

[367] 由此推出了 $\rho(F)\geqslant r$. 另外, 如果 $|z-z_0|<r$, 则

$$\sum_{n=0}^{+\infty}a_n(z-z_0)^n=\frac{1}{2i\pi}\sum_{n=0}^{+\infty}\int_{C(z_0,r)}\frac{(z-z_0)^nf(w)}{(w-z_0)^{n+1}}dw$$

---

[9]• 函数 $\varphi_0(x)=e^{-x^{-2}}$ 在连续延拓到 0 后属于 $\mathbf{R}$ 上的 $\mathscr{C}^\infty$ 类, 但在 0 附近却不能展开为整级数: 因为它在 0 的所有阶导数均为 0, 然而当 $x\neq 0$ 时却有 $\varphi_0(x)>0$.

• 函数 $\frac{1}{x^2+1}$ 在 $\mathbf{R}$ 上解析, 但在 $]-(1+\varepsilon),1+\varepsilon[,\varepsilon>0$ 上却不能展开为整级数: 因为在 0 的泰勒展开式 $\sum_{n=0}^{+\infty}(-x^2)^n$ 的收敛半径等于 1.

• 存在 $\mathbf{R}$ 上的连续函数但在每点都没有导数 (魏尔斯特拉斯,1875); 取此函数的原函数, 则证明了存在一个 $\mathbf{R}$ 上的 $\mathscr{C}^1$ 类函数但却不是 $\mathscr{C}^2$ 类的, 更不用说是解析的了.

另一方面, 全纯函数的理论在单实变函数理论前就已经发展起来了, 而正是后者的这些异常情形使得 19 世纪的数学家们大为惊讶 (也包括 20 世纪的一些人). 譬如, 庞加莱就对某些 $\mathscr{C}^\infty$ 类函数不是它们的泰勒级数的和感到烦恼.

$$= \frac{1}{2i\pi}\int_{C(z_0,r)}\sum_{n=0}^{+\infty}\frac{(z-z_0)^n f(w)}{(w-z_0)^{n+1}}dw = \frac{1}{2i\pi}\int_{C(z_0,r)}\frac{f(w)}{w-z}dw.$$

应用柯西积分公式便得结论.(对于上面交换 $\int$ 与 $\sum$ 的合理性, 譬如可以应用控制收敛定理: 在 $C(z_0,r)$ 上 $|\sum_{n=0}^{N}\frac{(z-z_0)^n f(w)}{(w-z_0)^{n+1}}|$ 被 $M\sum_{n=0}^{+\infty}\frac{|z-z_0|^n}{r^{n+1}} = \frac{M}{r-|z-z_0|}$ 控制.) □

推论 V.4.8. — (i) 如果在 Ω 上 f 全纯且不取零值, 则 $1/f$ 在 Ω 上全纯; 它的导数为 $\frac{-f'}{f^2}$.

(ii) 如果 $f:\Omega_1\to\Omega_2$ 全纯, 且 $g:\Omega_2\to\mathbf{C}$ 也全纯, 则 $g\circ f:\Omega_1\to\mathbf{C}$ 全纯; 其导数为 $(g'\circ f)f'$.

(iii) 如果 $f:\Omega_1\to\Omega_2$ 为全纯的双射, 且若其逆 $f^{-1}:\Omega_2\to\Omega_1$ 连续而且 f' 在 Ω 上不取零值[10], 则 f^{-1} 全纯; 其导数为 $\frac{1}{f'\circ f^{-1}}$.

证明　只需重复在实的情形时证明 $1/f$ (分别地, $g\circ f$; 分别地, f^{-1}) 是在 Ω (分别地, Ω_1; 分别地, Ω_2) 上属于复 $\mathscr{C}^1$ 即可: 命题 V.4.7 可以推出 $1/f$ (分别地, $g\circ f$; 分别地, f^{-1}) 的全纯性. (我们也可以直接证明 $1/f$ (分别地, $g\circ f$; 分别地, f^{-1}) 在每点附近可展开为整级数, 但这是相当耗费精力的.) □

5. 收敛半径和关于导数的柯西不等式

注记 V.4.9. — (i) 公式 $f(z)=F(z-z_0)$ 证明了这些 a_n 是 f 在 z_0 的泰勒展开式的系数. 换而言之, 在开集 Ω 上的一个全纯函数 f 在所有包含在 Ω 的开圆盘 $D(z_0,r^-)$ 上是它在 z_0 的泰勒级数的和. 另外, 如果 $D(z_0,r)\subset\Omega$, 则

$$\frac{1}{n!}f^{(n)}(z_0) = \frac{1}{2i\pi}\int_{C(z_0,r)}\frac{f(w)}{(w-z_0)^{n+1}}dw.$$

(ii) 在 $n=0$ 的情形得到了 $f(z_0)=\frac{1}{2\pi}\int_0^{2\pi}f(z_0+re^{i\theta})d\theta$, 这表明 f 满足平均性: $f(z_0)$ 是 $f(z)$ 在中心为 z_0 的整个圆上的平均值, 其中的圆所围成的圆盘包含在 Ω 中.

(iii) 在一般情形我们得到了控制强函数 (称作柯西不等式):

$$|\frac{1}{n!}f^{(n)}(z_0)| \leqslant r^{-n}\sup_{w\in C(z_0,r)}|f(z)| = r^{-n}\sup_{\theta\in[0,2\pi]}|f(z_0+re^{i\theta})|.$$

(iv) 更一般地, 如果 $K\subset\Omega$ 为紧集, 而 U 为包含 K 的开集, 使其闭包 $\overline{U}$ 为包含在 Ω 中的一个紧集[11], 于是对任意的 $n\in\mathbf{N}$, 存在 $M=M(n,K,U)$, 使得 [368]

$$\sup_{z\in K}|f^{(n)}(z)| \leqslant M\sup_{z\in\overline{U}}|f(z)|.$$

[10] 事实上, 这两个假设条件是不必要的 (参看注记 V.6.3 的第二个 •).

[11] 这样的开集总是有的: 由于 K 为紧集, 故有 $\delta=d(K,\mathbf{C}-\Omega)>0$; 设 $0<\delta'<\delta$, 则只要取 $U=\{z\in\mathbf{C}, d(z,K)<\delta'\}$ 即可; 由于 $z\mapsto d(z,K)$ 连续, 故它为开集, 又由于 $\delta'<\delta$, 故其闭包 $\overline{U}=\{z\in\mathbf{C}, d(z,K)\leqslant\delta'\}$ 包含在 Ω 中, 并且因为 K 有界故 $\overline{U}$ 为闭集, 有界, 从而也是一个紧集.

事实上, 如果 $r \leqslant d(K, \Omega - U)$, 则对任意的 $z \in K$ 有 $C(z,r) \subset \overline{U} \subset \Omega$, 那么 (i) 表明可取 $M = n! r^{-n}$.

命题 V.4.10. — 设 log 为对数主分支. 于是当 $|z| < 1$ 时有

$$\log(1+z) = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n} z^n.$$

证明 首先, 我们假设 $f(z) = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n} z^n$. 这是 $D(0,1^-)$ 上的全纯函数, 其导数为 $\sum_{n=1}^{+\infty} (-1)^{n-1} z^{n-1} = \frac{1}{1+z}$. 其次, $\log(1+z)$ 在 $D(0,1^-)$ 上也全纯, 其导数也为 $\frac{1}{1+z}$. 根据注记 V.4.9 的 (i), 函数 $g(z) = f(z) - \log(1+z)$ 在 $D(0,1^-)$ 上是它在 0 的泰勒级数的和, 而由于其导数为零, 又在 $D(0,1^-)$ 上为常值, 但 $g(0) = 0$, 故得结论. □

习题 V.4.11. — (i) 证明 $\tan = \frac{\sin}{\cos}$ 在 $]-\frac{\pi}{2}, \frac{\pi}{2}[$ 上是它的在 0 的泰勒级数的和.

(ii) $\frac{\tan z}{z^2+1}$ 在 0 的泰勒级数的收敛半径是多少?

(iii) $\frac{\sin \pi z}{z^2-1}$ 在 0 的泰勒级数的收敛半径是多少?

习题 V.4.12. — (i) 设 $s \in \mathbf{C}$. $(1+z)^s$ 的定义为 $(1+z)^s = \exp(s \log(1+z))$, 其中 log 是对数主分支. 证明 $(1+z)^s = \sum_{n=0}^{+\infty} \binom{s}{n} z^n, |z| < 1$.

(ii) 是否存在在 $D(0,1^-)$ 上的全纯函数 f, 使得在每个 $z \in D(0,1^-)$ 上 $f(z)^2 = z$?

习题 V.4.13. — 从均值定理推出极大值原理.

推论 V.4.14. — (刘维尔 (Liouville), 1844) 如果 f 是整个 $\mathbf{C}$ 上的有界的全纯函数, 则 f 为常数.

证明 由假设条件, 存在 $M > 0$ 使得对任意的 $z \in \mathbf{C}$ 有 $|f(z)| \leqslant M$. 由柯西不等式知, 如果 $n \in \mathbf{N}$, 则 $|\frac{1}{n!} f^{(n)}(0)| \leqslant r^{-n} M$, 其中 $r > 0$ 任意. 让 r 趋向 $+\infty$ 得到, 对于 $n \geqslant 1$ 有 $f^{(n)}(0) = 0$. 然而 f 在整个 $\mathbf{C}$ 上全纯, 从而在整个 $\mathbf{C}$ 上是其在 0 的泰勒级数的和, 因此对所有的 $z \in \mathbf{C}$ 有 $f(z) = f(0)$. 得证. □

推论 V.4.15. — (达朗贝尔–高斯定理, 1799) $\mathbf{C}$ 为代数闭域.

证明 设 $P \in \mathbf{C}[T]$ 在 $\mathbf{C}$ 上不取零值. 于是 $f = 1/P$ 是一个全纯函数. 但由于当 $|z| \to +\infty$ 时 f 有极限并且连续, 故 f 有界. 由刘维尔定理知 f 为常值从而 P 的次数为 0. 设若相反, 如果 $\deg P \geqslant 1$, 则 P 在 $\mathbf{C}$ 必有零点. 得证. □ [369]

习题 V.4.16. — 设 f 是整个 $\mathbf{C}$ 上的全纯函数. 假设存在 $N \in \mathbf{N}$ 和 $C > 0$ 使得对于所有的 $z \in \mathbf{C}$ 有 $|f(z)| \leqslant C|z|^N$. 证明 f 是一个多项式.

V.5. 构造全纯函数

1. 全纯函数的级数

设 Ω 为 $\mathbf{C}$ 的一个开集. 我们已经知道, 一个函数序列 $(f_n)_{n\in\mathbf{N}}$ 在 Ω 的所有紧集上一致收敛于 f 是指, 对于每个紧集 $K\subset\Omega$ 及每个 $\varepsilon>0$, 存在 $N(K,\varepsilon)$ 使得当 $z\in K$ 和 $n\geqslant N(K,\varepsilon)$ 时有 $|f_n(z)-f(z)|<\varepsilon$. 一个级数 $\sum_{n\in\mathbf{N}}u_n$ 在 Ω 的所有紧集上一致收敛是指它的部分和的序列在所有紧集上一致收敛; 它在 Ω 的所有紧集上按范数收敛是指, 对于每个紧集 $K\subset\Omega$ 有 $\sum_{n\in\mathbf{N}}\|u_n\|_K<+\infty$, 其中 $\|u_n\|_K=\sup_{z\in K}|u_n(z)|$ 是 u_n 在 K 上的一致收敛范数.

在所有紧集上按范数的收敛性蕴含了所有紧集上的一致收敛性, 而它则蕴含了单收敛性.

定理 V.5.1. — 设 Ω 是 $\mathbf{C}$ 的一个开集.

(i) 如果 $(f_n)_{n\in\mathbf{N}}$ 是 Ω 上的全纯函数序列, 它在 Ω 的所有紧集上一致收敛, 则序列 f_n 的极限 f 在 Ω 上全纯, 并且对所有的 k, 序列 $(f_n^{(k)})_{n\in\mathbf{N}}$ 在 Ω 的每个紧集上一致收敛于 $f^{(k)}$.

(ii) 如果 $(u_n)_{n\in\mathbf{N}}$ 是 Ω 上的全纯函数序列使得级数 $\sum_{n\in\mathbf{N}}u_n$ 在 Ω 的每个紧集上一致 (分别地, 按范数) 收敛, 则该级数的和在 Ω 上全纯, 并对所有的 k, 级数 $\sum_{n\in\mathbf{N}}u_n^{(k)}$ 在 Ω 的每个紧集上一致 (分别地, 按范数) 收敛于 $f^{(k)}$.

证明 (i) 由 (ii) 得到, 而要证明 (ii) 只要证明 f 全纯即可, 其余的用上面注记 V.4.9 的 (iv) 就可得到.

设 $z_0\in\Omega$ 且 $r>0$, 使得 $D(z_0,r)\subset\Omega$. 于是根据柯西公式, 对每个 $z\in K$ 有

$$\begin{aligned}f(z)=\sum_{n\in\mathbf{N}}u_n(z)&=\frac{1}{2i\pi}\sum_{n\in\mathbf{N}}\int_{C(z_0,r)}\frac{u_n(w)}{w-z}dw\\&=\frac{1}{2i\pi}\int_{C(z_0,r)}\sum_{n\in\mathbf{N}}\frac{u_n(w)}{w-z}dw=\frac{1}{2i\pi}\int_{C(z_0,r)}\frac{f(w)}{w-z}dw,\end{aligned}$$

上式中用到符号 $\int$ 与 $\sum$ 的互换的合理性来自级数在紧集 $C(z_0,r)$ 上的一致 (分别地, 按范数) 收敛性. 命题 V.4.7 让我们推出 f 在 $D(z_0,r^-)$ 上的全纯性. 证完. □

习题 V.5.2. — 设 Ω 是 $\mathbf{C}$ 的一个开集, 而 $(f_n)_{n\in\mathbf{N}}$ 是 Ω 上单趋向 f 的全纯函数的序列. 证明, 如果对于 Ω 的每个紧集 K, 存在 $M_K>0$ 使得对于所有的 $n\in\mathbf{N}$ 和 $z\in K$ 有 $|f_n(z)|\leqslant M_K$, 则 f 全纯. [370]

习题 V.5.3. — (i) 证明级数 $\sum_{n=N+1}^{+\infty}(\frac{1}{z+n}+\frac{1}{z-n})$ 在 $D(0,(N+\frac{1}{2})^-)$ 上一致收敛. 由此得到 $z\mapsto F(z)=\frac{1}{2}+\sum_{n=1}^{+\infty}(\frac{1}{z+n}+\frac{1}{z-n})$ 在 $\mathbf{C}-\mathbf{Z}$ 上全纯.

(ii) 证明 $G(z)=F(z)-\pi\cot\pi z$ 为周期为 1 的奇周期函数.

(iii) 证明 G 可连续延拓为 $\mathbf{C}$ 上的一个全纯函数.

(iv) 证明 G 在 $\mathbf{C}$ 上有界; 由此得到, 当 $z \in \mathbf{C}-\mathbf{Z}$ 时有 $\frac{1}{2}+\sum_{n=1}^{+\infty}(\frac{1}{z+n}+\frac{1}{z-n}) = \pi\cot\pi z$.

(v) 设 $\sum_{n=0}^{+\infty} B_n \frac{t^n}{n!}$ 是 $\frac{t}{e^t-1}$ 在 $t=0$ 的泰勒展开式, 并设为 $k \geqslant 1$ 的整数, 而 $\zeta(2k)=\sum_{n=1}^{+\infty}\frac{1}{n^{2k}}$. 证明

$$\zeta(2k) = -\frac{1}{2}B_{2k}\frac{(2i\pi)^{2k}}{(2k)!}.$$

由此得到 $\pi^{-2k}\zeta(2k)$ 是一个有理数 (欧拉, 1731).

2. 全纯函数的无限乘积

设 I 是一个可数集, 而 $(u_n)_{n\in I}$ 是一个复数的序列. 称乘积 $\prod_{i\in I} u_i$ 收敛是说 $\sum_{i\in I}|u_i-1| < +\infty$. 如果对于所有的 $i \in I$ 有 $u_i \neq 0$, 此条件则等价于 $\sum_{i\in I}|\log u_i| < +\infty$, 其中 $\log : \mathbf{C}^* \to \mathbf{C}$ 代表虚部属于 $]-\pi,\pi]$ 的对数分支 (特别地, 当 $|z-1|<1$ 时, $\log z = \sum_{n=1}^{+\infty}\frac{(-1)^{n-1}}{n}(z-1)^n$, 并且 $\lim_{z\to 1}\frac{\log z}{z-1}=1$). 如果 I 有限, 此乘积总收敛, 它的值是通常的乘积, 如果 I 无限, 且若 $n \mapsto i(n)$ 是一个从 $\mathbf{N}$ 到 I 的双射, 这时 $x_n = \prod_{k\leqslant n} u_{i(k)}$ 是一个收敛的序列, 则它的极限不依赖从 $\mathbf{N}$ 到 I 的双射的选取, 它便定义为这个无限乘积的值. 事实上:

- 如果存在 i 使得 $u_i = 0$, 则对充分大的 n, $x_n = 0$, 故此乘积为 0.
- 如果对所有的 i, $u_i \neq 0$, 则有 $x_n = \exp(\sum_{k\leqslant n}\log u_{i(k)})$, 而因为 $\sum_{i\in I}|\log u_i| < +\infty$, 级数 $\sum_{n\in\mathbf{N}}\log u_{i(n)}$ 收敛, 从而 $\prod_{i\in I} x_i = \exp(\sum_{n\in\mathbf{N}}\log u_{i(n)}) = \exp(\sum_{i\in I}\log u_i)$.

特别地, 一个收敛的乘积为 0 当且仅当该乘积中有一项为 0.

定理 V.5.4. — 设 Ω 是 $\mathbf{C}$ 的一个开集, 且设 $(u_n)_{n\in\mathbf{N}}$ 是 Ω 上的一个全纯函数的序列, 使得级数 $\sum_{n\in\mathbf{N}} u_n$ 在 Ω 的所有紧集上按范数收敛, 又令 $f_n = \prod_{k=0}^{n}(1+u_k)$, $n\in\mathbf{N}$.

(i) 序列 f_n 在所有紧集上一致收敛 (这时称无限乘积 $\prod_{n\in\mathbf{N}}(1+u_n)$ 在所有紧集上一致收敛), 而序列 f_n 的极限 f 在 Ω 上全纯.

(ii) 如果 Ω 连通, 并且没有一个 u_n 在 Ω 上恒等于 -1, 则 $f(z)=0$ 当且仅当存在 $n\in\mathbf{N}$ 使得 $1+u_n(z)=0$, 且对任意的 $z\in\Omega$ 有 $v_z(f)=\sum_{n\in\mathbf{N}} v_z(1+u_n)$. 又, 级数 $\sum_{n=0}^{+\infty}\frac{u_n'}{1+u_n}$ 在 Ω 的使 f 不取 0 的紧集上按范数收敛, 而且 [371]

$$\frac{f'(z)}{f(z)} = \sum_{n=0}^{+\infty}\frac{u_n'(z)}{1+u_n(z)},\ f(z)\neq 0.$$

证明 如果 K 是 Ω 的一个紧集, 令 $C(K)=\exp(\sum_{n\in\mathbf{N}}\|u_n\|_K)$; 根据假设知这是一个有限数. 如果 $n\in\mathbf{N}$ 且 $z\in K$, 于是有

$$\begin{aligned}|\prod_{k=0}^{n+1}(1+u_k(z)) - \prod_{k=0}^{n}(1+u_k(z))| &= |u_{n+1}(z)|\cdot|\prod_{k=0}^{n}(1+u_k(z))| \\ &\leqslant \|u_{n+1}\|_K\prod_{k=0}^{n}(1+\|u_k\|_K) \leqslant C(K)\|u_{n+1}\|_K.\end{aligned}$$

由此, 并由于 $\sum_{n\in\mathbf{N}}\|u_n\|_K$ 的收敛性, 得到在 K 上此乘积的一致收敛性. 根据定理 V.5.1 知, 极限 f 在 Ω 上全纯.

现在, 如果 $z_0\in\Omega$, 则可选取 $r>0$ 使得 $K=D(z_0,r)\subset\Omega$ 及 $N\in\mathbf{N}$ 使得 $\|u_n\|_K\leqslant\frac{1}{2}$, 其中 $n>N$. 特别地, $1+u_n$ 在 K 上不取 0, 并且对所有 $z\in K=D(z_0,r)$ 有 $|1+u_n(z)|\geqslant 1-\|u_n\|_K\geqslant e^{-2\|u_n\|_K}$. 设 $g_N=\prod_{n\geqslant N+1}(1+u_n)$. 从上面便得到了控制不等式 $|g_N(z)|\geqslant\exp(-2\sum_{n=N+1}^{+\infty}\|u_n\|_K)$, 这便证明了 g_N 在 K 上不取 0. 由此推出

$$v_{z_0}(f)=v_{z_0}(g_N\prod_{n=0}^{N}(1+u_n))=\sum_{n=0}^{N}v_{z_0}(1+u_n)=\sum_{n=0}^{+\infty}v_{z_0}(1+u_n).$$

u_n 的级数按范数收敛性, 根据定理 V.5.1 的 (ii), 因而蕴含了 u_n' 的级数的按范数的收敛性. 由于当 $z\in K$ 和 $n\geqslant N$ 时有 $|1+u_n(z)|\geqslant\frac{1}{2}$, 由此得到 $\frac{u_n'}{1+u_n}$ 的级数也按范数收敛. 同样, f_n 在 K 上一致收敛于 f 给出了 f_n' 也如此地收敛于 f' (定理 V.5.1 的 (i)). 我们因此得到 $\frac{f_n'(z)}{f_n(z)}$ 在 $f(z)\neq 0$ 时趋向 $\frac{f'(z)}{f(z)}$. 然而 $\frac{f_n'}{f_n}=\sum_{k=0}^{n}\frac{u_k'}{1+u_k}$ (这可以从 $(v_1v_2)'=v_1'v_2+v_1v_2'$ 归纳得到), 从而当 $f(z)\neq 0$ 时有 $\frac{f'(z)}{f(z)}=\sum_{n=0}^{+\infty}\frac{u_n'(z)}{1+u_n(z)}$. 得到结论. □

习题 V.5.5. — 利用 $\log u_n$ 的级数重新证明此定理 (注意到 $\log u_n$ 不必是在整个 Ω 上全纯的).

习题 V.5.6. — 证明 $\prod_{n\geqslant 1}(1-\frac{z^2}{n^2})$ 在 $\mathbf{C}$ 的所有紧集上一致收敛, 并且其值为 $\frac{\sin\pi z}{\pi z}$. (利用习题 V.5.3 的结果; 参看习题 H.1.10 中另外的方法.)

3. 积分定义的全纯函数

定理 V.5.7. — 设 X 是 $\mathbf{R}^m$ 中的一个可测子集, 而 Ω 是 $\mathbf{C}$ 的一个开集. 设 $F:\Omega\times X\to\mathbf{C}$. 假设:

- $z\mapsto F(z,t)$ 对于任意的 $t\in X$ 是 Ω 上的全纯函数,
- $t\mapsto F(z,t)$ 对于任意的 $z_0\in\Omega$ 是可测函数, 并且存在 $r_{z_0}>0$ 和 $g_{z_0}\in\mathscr{L}^1(X)$ 使得 $D(z_0,r_{z_0})\subset\Omega$ 和对所有 $z\in D(z_0,r_{z_0})$ 及 $t\in X$ 有 $|F(z,t)|\leqslant g_{z_0}(t)$.

于是定义为 $f(z)=\int_X F(z,t)dt$ 的函数 $f:\Omega\to\mathbf{C}$ 在 Ω 上全纯. 又, 如果 $k\in\mathbf{N}$, 则 $(\frac{\partial}{\partial z})^k f(z)=\int_X(\frac{\partial}{\partial z})^k F(x,t)dt$. [372]

证明 全纯是一个局部性质, 故只要证明对任意的 $z_0\in\Omega$, 存在 $r>0$ 使得 f 在 $D(z_0,r^-)$ 上全纯即可. 那么取定一个 $z_0\in\Omega$ 并设 $r=r_{z_0}$. 由于 $z\mapsto F(z,t)$ 对任意 $t\in X$ 全纯, 我们可由柯西公式得到恒等式

$$f(z)=\frac{1}{2i\pi}\int_X\left(\int_{C(z_0,r)}\frac{F(w,t)}{w-z}dw\right)dt,$$

其中 $z\in D(z_0,r^-)$. 但如果 $(w,t)\in(C(z_0,r)\times X)$, 则有 $|\frac{F(w,t)}{w-z}|\leqslant\frac{g_{z_0}(t)}{r-|z-z_0|}$. 由于 g_{z_0} 在 X 上可和, 故函数 $|\frac{F(w,t)}{w-z}|$ 在 $C(z_0,r)\times X$ 上可和, 因此可以应用富比尼定理

来交换这两个积分. 于是得到

$$f(z)=\frac{1}{2i\pi}\int_{C(z_0,r)}\left(\int_X\frac{F(w,t)}{w-z}dt\right)dw=\frac{1}{2i\pi}\int_{C(z_0,r)}\frac{f(w)}{w-z}dw,$$

其中 $z\in D(z_0,r^-)$. 命题 V.4.7 让我们能推出 f 在 $D(z_0,r^-)$ 上全纯.

现在根据注记 V.4.9, 我们有 $\frac{1}{k!}f^{(k)}(z_0)=\frac{1}{2i\pi}\int_{C(z_0,r)}\frac{f(w)}{(w-z_0)^{k+1}}dw$. 以 $r^{-k-1}g_{z_0}(t)$ 为强函数控制 $|\frac{f(w)}{(w-z_0)^{k+1}}|$, 而此强函数在 $C(z_0,r)\times X$ 上可和, 从而使我们能在另一方向上应用富比尼定理, 得到了

$$\frac{1}{k!}f^{(k)}(z_0)=\int_X\left(\frac{1}{2i\pi}\int_{C(z_0,r)}\frac{F(w,t)}{(w-z_0)^{k+1}}dw\right)dt=\int_X\frac{1}{k!}\left(\frac{\partial}{\partial z}\right)^kF(z_0,t)dt.$$

即为所证. □

推论 V.5.8. — 设 Ω 和 D 为 $\mathbf{C}$ 的两个开集. 如果 f 在 $\Omega\times D$ 上连续, 且若 $z\mapsto f(z,w)$ 对于每一个 $w\in D$ 在 Ω 上全纯, 则对于包含在 D 中的分段 $\mathscr{C}^1$ 的道路 γ, $z\mapsto\int_\gamma f(z,w)dw$ 全纯.

证明 我们有 $\int_\gamma f(z,w)dw=\int_0^1 f(z,\gamma(t))\gamma'(t)dt$. 设 $z_0\in\Omega$. 于是可以找到 $r>0$ 使得 $D(z_0,r)\subset\Omega$. 连续函数 $(x,t)\mapsto|f(z,\gamma(t))|$ 在紧集 $D(z_0,r)\times[0,1]$ 上被 M 控制, 从而 $f(z,\gamma(t))\gamma'(t)$ 在 $D(z_0,r)\times[0,1]$ 上被形如 $M|\gamma'(t)|$ 的函数控制. 由于 $\int_0^1|\gamma'(t)|dt<+\infty$, 从而满足定理 V.5.7 的条件. 得证. □

习题 V.5.9. — (复平面上的 Γ 函数)

(i) 证明 $F(z)=\int_0^{+\infty}e^{-t}t^z\frac{dt}{t}$ 当 $\mathrm{Re}(z)>0$ 时收敛, 而 $z\mapsto F(z)$ 在半平面 $\mathrm{Re}(z)$ 上全纯.

(ii) 证明对于任意的 $n\in\mathbf{N}$ 有 $F(z)=\frac{F(z+n+1)}{z(z+1)\cdots(z+n)}$, 其中 $\mathrm{Re}(z)>0$. 因此得到, 存在唯一的函数 Γ, 它在 $\mathbf{C}-(-\mathbf{N})$ 上全纯, 并在负整数上具有单极点, 使得当 $\mathrm{Re}(z)>0$ 时有 $\Gamma(z)=F(z)$.

[373] (iii) 证明 $F(z)$ 在整个竖直的带状区域 $0<a<\mathrm{Re}(z)\leqslant b<+\infty$ 上有界; 因此推出 Γ 在有限宽的竖直带的无限远处速降, 就是说, 对于任意 $a<b\in\mathbf{R}$ 和 $N\in\mathbf{N}$, 存在 $C(a,b,N)$ 使得

$$|\Gamma(z)|\leqslant C(a,b,N)|\mathrm{Im}(z)|^{-N},$$

其中 $a\leqslant\mathrm{Re}(z)\leqslant b$ 且 $|\mathrm{Im}(z)|\geqslant 1$.

V.6. 全局逆和开的像

1. 全纯函数的局部逆定理

设 Ω_1,Ω_2 是 $\mathbf{C}$ 的两个开集. 称映射 $\varphi:\Omega_1\to\Omega_2$ 为双全纯的是说, 它是一个双射, 并且 φ 和 φ^{-1} 都为全纯的. (我们将在后面 (注记 V.6.3) 看到, 只要 φ 为单的且

全纯的它就是双全纯的.

定理 V.6.1. — (对于全纯函数的局部逆) 设 Ω 是 $\mathbf{C}$ 的开集, 而 f 在 Ω 上全纯, 且 $z_0\in\Omega$. 如果 $f'(z_0)\neq 0$, 则存在 z_0 在 Ω 中的一个开邻域 U 及 $f(z_0)$ 在 $\mathbf{C}$ 中的一个开邻域 V, 使得 f 是从 U 到 V 的双全纯.

证明　首先假设 $z_0=0, f(z_0)=0$ 且 $f'(z_0)=1$; 我们将用不动点的方法构造 f 的逆映射 g (参看小词典的 14.2 小节): 出发点是, g 是 $\varphi\mapsto\varphi-f\circ\varphi+\mathrm{id}$ 的不动点.

存在 $\alpha\in\mathbf{C}$ 使得 $f(z)=z+\alpha z^2+O(|z|^3)$, 于是

$$h(u,v)=f(u-v)-f(u)+v=\alpha(v^2-2uv)+O((|u|+|v|)^3).$$

设 $r_0<\frac{1}{2}\rho(f)$. 从上面的有限展开式得知, 存在 $C>0$ 使得当 $|v|\leqslant|u|\leqslant r_0$ 时有 $|h(u,v)|<C|u|\cdot|v|$. 由于 $f(z)-z=O(|z|^2)$, 如有必要可减小 r_0, 故可进一步假设当 $|z|\leqslant r_0$ 时有 $|f(z)-z|\leqslant\frac{1}{4}|z|$, 并且也可令 $r_0\leqslant\frac{1}{2C}$.

设 $r=\frac{2}{3}r_0$. 由归纳构造两个函数序列 $(g_n)_{n\geqslant1}$ 和 $(u_n)_{n\geqslant1}$ 如下: 令 $g_1(z)=z; u_n(z)=f(g_n(z))-z; g_{n+1}(z)=g_n(z)-u_n(z)$. 我们要证明 g_n 和 u_n 在 $D(0,r^-)$ 上全纯, 并且对任意的 $z\in D(0,r^-)$ 有

$$\left(\frac{1}{2}+\frac{1}{2^n}\right)|z|\leqslant|g_n(z)|\leqslant\left(\frac{3}{2}-\frac{1}{2^n}\right)|z|\quad\text{和}\quad|u_n(z)|\leqslant\frac{1}{2^{n+1}}|z|.$$

由于 $g_1(z)=z$ 而 $u_1(z)=f(z)-z$, 故上面公式对于 $n=1$ 显然成立. 如果此结果对于 n 满足, 则 $|g_{n+1}(z)|$ 的两端的界限立即由 $|g_n(z)|$ 的界限和 $|u_n(z)|$ 的那个限制强函数得到. 另外, 由于 $|g_{n+1}(z)|\leqslant\frac{2}{3}|z|<r_0<\rho(f)$, 则函数 $z\mapsto f(g_{n+1}(z))$ 有定义, 并且在 $D(0,r^-)$ 上全纯, 因此 u_{n+1} 在 $D(0,r^-)$ 上全纯. 现在,

$$u_{n+1}(z)=f(g_n(z)-u_n(z))-z=h(g_n(z),u_n(z))+f(g_n(z))-u_n(z)-z=h(g_n(z),u_n(z)),$$

由于 $|u_n(z)|\leqslant\frac{1}{2^{n+1}}|z|\leqslant(\frac{1}{2}+\frac{1}{2^n})|z|\leqslant|g_n(z)|$, 故有

$$|u_{n+1}(z)|\leqslant|h(g_n(z),u_n(z))|\leqslant C|g_n(z)||u_n(z)|\leqslant\frac{3C|z|}{2}\cdot\frac{|z|}{2^{n+1}}\leqslant Cr_0\frac{|z|}{2^{n+1}}\leqslant\frac{|z|}{2^{n+2}}.$$

这证明了归纳假定当 $n+1$ 时也满足.

从控制关系 $|g_{n+1}(z)-g_n(z)|=|u_n(z)|\leqslant\frac{r}{2^{n+1}}$ 推出了序列 g_n 在 $D(0,r^-)$ 上的一致收敛性. 它的极限因此是 $D(0,r^-)$ 上的全纯函数, 并满足 $g(z)=g(z)-(f(g(z))-z)$. 换句话说, 我们已经构造了 $D(0,r^-)$ 上的一个全纯函数 g 使得当 $z\in D(0,r^-)$ 时有 $f(g(z))=z$.

在一般情形, 可应用前面的结果到 $F(z)=f'(z_0)^{-1}(f(z+z_0)-f(z_0))$ 上 (从而 $f(z)=f'(z_0)(F(z-z_0)+f(z_0))$. 由此可知, 存在 $r_0>0$ 以及在 $D(0,r_0^-)$ 上全纯的 G 使得当 $z\in D(0,r_0^-)$ 时有 $F(G(z))=z$. g 在 $D(f(z_0),r^-)$ 上定义为 $g(z)=z_0+G(f'(z_0)^{-1}(z-f(z_0)))$, 其中 $r=|f'(z_0)|r_0$; 做一点计算立即证明了当 [374]

$z \in D(f(z_0), r^-)$ 时有 $f(g(z)) = z$. 换句话说, 我们可以找到 $f(z_0)$ 的一个开邻域 V_0 以及在 V_0 上全纯的 g 使得在 V_0 上 $f \circ g = \text{id}$. 这特别表明 g 在 V_0 上是一个单射. 另外, 当 $z \in V_0$ 时还有 $f'(g(z))g'(z) = 1$, 从而 $g(f(z_0)) \neq 0$. 将前面对 f 的结果用到 g, 则得知存在 z_0 的一个邻域 U(包含在 Ω 中) 和全纯的 $h : U \to V_0$, 使得在 U 上 $g \circ h = \text{id}$. 令 $V = h(U)$. 由于在 U 上 $g \circ h = \text{id}$, 故 $g(V) = U$, 又由于 g 在 V_0 上为单射, 因而有 $V = g^{-1}(U)$, 这证明了 V 是一个包含 $z_0 = h(f(z_0))$ 的开集 (V 在 V_0 中, 而 V_0 在 $\mathbf{C}$ 中, 从而 V 在 $\mathbf{C}$ 中). 最后, 我们有 $f = f \circ (g \circ h) = (f \circ g) \circ h = h$ 在 U 中, 且 $f \circ g = \text{id}$ 在 V 中 ($\text{V} \subset \text{V}_0$) 且 $g \circ f = g \circ h = \text{id}$ 在 U 中. f 诱导了从 U 到 V 上的一个全纯的双射, 而其逆 g 也全纯. 证完. □

2. 全纯函数的局部结构

定理 V.6.2. — 设 Ω 是 $\mathbf{C}$ 的一个连通开集, 而 f 是 Ω 上的一个非常值的全纯函数. 如果 $z_0 \in \Omega$ 及 $m = v_{z_0}(f - f(z_0))$, 则存在在 z_0 在 Ω 中的一个邻域 U 和一个实数 $r > 0$, 以及一个满足 $\varphi(z_0) = 0$ 的双全纯映射 $\varphi : U \to D(0, r^-)$, 使得对任意的 $z \in U$ 有 $f(z) = f(z_0) + \varphi(z)^m$.

证明 由 m 的定义知, 在 z_0 的一个邻域有

$$f(z) - f(z_0) = (z - z_0)^m (a_m + a_{m+1}(z - z_0) + \cdots),$$

其中 $a_m \neq 0$. 设 $\alpha \in \mathbf{C}^*$ 是 a_m 的一个 m 次根, 并令

$$g = \frac{f(z) - f(z_0)}{a_m (z - z_0)^m} = 1 + b_1(z - z_0) + \cdots .$$

函数 g 在 U_0 中全纯, 且由于它在 z_0 取值 1, 故存在 z_0 的一个邻域 U_1, 使得当 $z \in U_1$ 时有 $g(z) \in D(1, 1^-)$. 然而由此知函数 $h = g^{1/m}$ 在 U_1 上全纯并满足 $h^m = g$ (参看注记 V.1.8). 这证明了, 如果令 $\varphi(z) = \alpha(z - z_0)h(z)$, 则 φ 在 U_1 上全纯, 并对任意的 $z \in U_1$ 有 $f(z) = f(z_0) + \varphi(z)^m$. 最后, 由于 $\varphi'(z_0) = \alpha \neq 0$, 全纯的局部逆定理表明存在 z_0 的在 U_0 中的开邻域 U 及 $r > 0$, 使得 φ 诱导了从 U 到 $D(0, r^-)$ 的一个双全纯的双射. □

注记 V.6.3. — 如果 $m \geqslant 1$, 映射 $z \mapsto z^m$ 诱导了从 $D(0, r^-)$ 到 $D(0, (r^m)^-)$ 上的一个满射, 而 $D(0, (r^m)^-) - \{0\}$ 的每个点正好有 m 个原像. 由此得到 (由于定理 V. 6.2) 下面的结果.

- 如果 Ω 是 $\mathbf{C}$ 的一个开集, 且 f 是 Ω 上的一个非常值的全纯函数, 则 $f(\Omega)$ 是一个开集 (开映射定理). 事实上, 仍旧使用定理中的记号则可以看出, 如果 $z_0 \in \Omega$, 则存在 $r > 0$ 使得 $f(\Omega)$ 包含了 $D(f(z_0), (r^m)^-)$. 它改进了最大值原理.

• 如果 Ω 是 $\mathbf{C}$ 的一个开集, 且 f 是 Ω 上的一个全纯的单射, 则 f 是 Ω 到 $f(\Omega)$ 上的双全纯映射 (整体逆命题). 事实上, 如果 f 为单射, 那么以定理中的记号, 应该有 $m = 1$[12], 而 f' 在 Ω 上不取零. 从局部逆定理得到 f^{-1} 在开集 $f(\Omega)$ 的每一个点的邻域中全纯. [375]

习题 V.6.4. — 证明不存在双射的全纯函数 $f : D(0, 1^-) \to \mathbf{C}$.

[12] 如果 $m \geqslant 2$ 且 $0 < |u - f(z_0)| < r^m$, 则 u 在 U 中有 m 个 f 的原像, 即在 φ 下 $u - f(z_0)$ 的 m 个 m 次根的逆像.

VI. 柯西公式和 (柯西) 留数公式

[377]

想必读者已感受到了在研讨全纯函数时柯西公式的强大威力. 作为该公式推广的留数公式则一方面是轻松计算某些积分的实用工具, 另一方面是极其灵活的理论性的工具, 我们将在第 VII 章和附录 A 中应用它. 另外, 它的运作思想则是更广泛地构建任意维流形的不变量的一个出发点. 例如, 可以利用留数公式 (及其中涉及的想法) 证明 $\mathbf{R}^2$ 的一个开集不同胚于 $\mathbf{R}^n, n \neq 2$ 中的一个开集. 证明 $\mathbf{R}^n$ 中的一个开集不同胚于 $\mathbf{R}^m, n \neq m$ 中的一个开集则 (极大地) 推广了这些思想 (这对于拓扑观点的维数概念是至关重要的).

VI.1. 闭道的同伦和柯西公式

1. 代数拓扑的术语

设 X 和 Y 为拓扑空间, 而 $f: X \to Y$ 和 $g: X \to Y$ 是两个连续映射. 称 f 和 g 是同伦的是说, 如果 "能够从 f 连续地过渡到 g". 准确地说, f 和 g 是同伦的是指存在连续的 $u: [0,1] \times X \to Y$, 使得对任意的 x 有 $u(0,x) = f(x)$ 而 $u(1,x) = g(x)$. 如果以 $f_t: X \to Y$ 记映射 $x \mapsto f_t(x) = u(t,x)$, 则 f_t 对于每个 $t \in [0,1]$ 连续, 而 $t \mapsto f_t$ 是从 $[0,1]$ 到 $X \to Y$ 的连续映射的空间 (赋予单收敛的拓扑) 的连续映射, 它将 $f = f_0$ 连接到 $g = f_1$.

$\mathbf{C}$ 的一个开集 Ω 是*可缩的*是指它同伦于一个点, 就是说, 存在 $z_0 \in \Omega$, 使得 $\mathrm{id}: \Omega \to \Omega$ 在 Ω 中同伦于常值映射 $z \mapsto z_0$, 其中 $z \in \Omega$ 任意. 换句话说, Ω 是可缩的是指存在 $z_0 \in \Omega$ 及连续的 $u: [0,1] \times \Omega \to \Omega$ 使得对任意的 $z \in \Omega$ 有 $u(0,z) = z$ 而 $u(1,z) = z_0$.

称一个开集 Ω 是*星形的*是说, 存在 $z_0 \in \Omega$ 使得对任意的 $z \in \Omega$, 线段 $[z_0, z]$

包含在 Ω 中. 特别地, 一个凸开集是一个星形; $\mathbf{C}$ 去掉一条半直线是星形的 (可
[378] 取 z_0 为在包含 Y 的直线的另一半上的任一点). 一个开星形是可缩的: 只要令 $u(t,z)=z(1-t)+tz_0$ 即可; 条件 $[z_0,z]\subset\Omega$ 使得 u 在 Ω 上取值.

如果 Ω 是 $\mathbf{C}$ 的一个开集, 一个从 $\gamma_0:(\mathbf{R}/\mathbf{Z})\to\Omega$ 到 $\gamma_1:(\mathbf{R}/\mathbf{Z})\to\Omega$ 上在 Ω 中的闭道的同伦是一个连续映射 : $u:[0,1]\times(\mathbf{R}/Z)\to\Omega$, 它满足 $u(0,t)=\gamma_0(t)$ 而 $u(1,t)=\gamma_1(t)$; 我们也可将 u 看作一个连续映射 $u:[0,1]\times[0,1]$ 使得对所有 $s\in[0,1]$ 有 $u(s,0)=u(s,1)$. 称闭道 $\gamma:(\mathbf{R}/\mathbf{Z})\to\Omega$ 在 Ω 中可缩是说, 存在一个从闭道 γ 到一个常闭道的同伦. 如果 Ω 可缩(1), 则 Ω 中所有闭道在 Ω 中均可缩.

2. 斯托克斯公式的一个特殊情形

设 $A=(0,0),B=(1,0),C=(1,1),D=(0,1)$ 为正方形 $[0,1]^2$ 的顶点. 以 $\partial([0,1]^2)$ 代表正方形 $[0,1]^2$ 的定向边界; 这是线段 $[A,B],[B,C],[C,D],[D,A]$ 的并.

命题 VI.1.1. — 如果 $\omega=Pds+Qdt$ 是 $[0,1]^2$ 上的一个 1-形式, 其中 P,Q 属于 $\mathscr{C}^1$ 类, 于是(2)

$$\int_{\partial([0,1]^2)}\omega=\int_{[0,1]^2}\left(-\frac{\partial P}{\partial t}+\frac{\partial Q}{\partial s}\right)dsdt.$$

证明 返回曲线积分的定义, 得到

$$\int_{[A,B]}\omega=\int_0^1 P(s,0)ds,\quad \int_{[C,D]}\omega=\int_0^1 P(1-v,1)dv=-\int_0^1 P(s,1)ds,$$
$$\int_{[B,C]}\omega=\int_0^1 Q(1,t)dt,\quad \int_{[D,A]}\omega=\int_0^1 Q(0,1-v)dv=-\int_0^1 Q(0,t)dt.$$

[379] 它们给出了

---

(1)更一般地, 一个连通的拓扑空间是单连通的是说 X 中所有的闭道均可缩. 根据黎曼 (1851) 宣布而由 P.Koebe (1914) 真正证明的著名定理 (黎曼的共形表示定理), $\mathbf{C}$ 的一个单连通的且不等于 $\mathbf{C}$ 的开集双全纯于一个单位元盘 $D=D(0,1^-)$. 特别地, 这使我们可以证明 $\mathbf{R}^2$ 的每一个单连通开集 U 均微分同胚于 $\mathbf{R}^2$ (即存在从 U 到 $\mathbf{R}^2$ 的 $\mathscr{C}^1$ 类双射, 并且其逆也属于 $\mathscr{C}^1$ 类). 由于一个全纯函数保持角不变, 我们看到, 可以在保持角不变时, 将一个元 (的内部) 变换成一个三角形 (的内部)……

(2)后面的公式是斯托克斯公式 $\int_\Omega d\omega=\int_{\partial\Omega}\omega$ 的一个特殊情形, 这是最美的也是最有用的数学公式之一. 在斯托克斯公式中, ω 是在 $p+1$ 维紧集 K 上的一个 p-形式, 而 $d\omega$ 是其微分, Ω 是 K 的内核, 而 $\partial\Omega$ 是 Ω 的定向边界 (从而也是 K 的). 要给出上面所说的准确意义需要再做点工作 (特别地, 要定义边界上的定向, 而这一般并不总能做到). 如果 $p=0$, 则斯托克斯公式就是 "分析基本定理" $\int_a^b df=f(b)-f(a)$, 而如果 $p=1$ 且 Ω 的维数等于 2, 则斯托克斯公式也以格林定理为名而为人所知 (因此有 $d(Pdx+Qdy)=dP\wedge dx+dQ\wedge dy=(-\frac{\partial P}{\partial y}+\frac{\partial Q}{\partial x})dx\wedge dy$, 这里的 $\wedge$ 是交错双线性的); 因此便回到了命题中的公式了.

$$\begin{aligned}\int_{\partial([0,1]^2)}\omega &= \int_0^1 (P(s,0)-P(s,1))ds + \int_0^1 (Q(1,t)-Q(0,t))dt \\ &= -\int_0^1 \left(\int_0^1 \frac{\partial P}{\partial t}(s,t)dt\right)ds + \int_0^1 \left(\int_0^1 \frac{\partial Q}{\partial s}(s,t)ds\right)dt \\ &= \int_{[0,1]^2} (\frac{-\partial P}{\partial t} + \frac{\partial Q}{\partial s})dsdt.\end{aligned}$$

□

如果 Ω 是 $\mathbf{C}$ 的一个开集, 又如果 $u:[0,1]^2 \to \Omega$ 是一个 $\mathscr{C}^1$ 类的映射, 而 $f:\Omega \to \mathbf{C}$ 也是 $\mathscr{C}^1$ 类的, 则用下面的公式定义 $[0,1]^2$ 上的一个 1-形式 $u^*(f(z)dz)$ 为:

$$u^*(f(z)dz) = f(u(s,t))d(u(s,t)) = f(u(s,t))\left(\frac{\partial u}{\partial s}(s,t)ds + \frac{\partial u}{\partial t}(s,t)dt\right).$$

引理 VI.1.2. — 设 Ω 是 $\mathbf{C}$ 的一个开集. 如果 $f:\Omega\to\mathbf{C}$ 是复 $\mathscr{C}^1$ 类函数, 而 $u:[0,1]^2\to\Omega$ 是一个 $\mathscr{C}^2$ 类的映射, 再令 $u^*(f(z)dz) = P(s,t)ds + Q(s,t)dt$, 则 $-\frac{\partial P}{\partial t} + \frac{\partial Q}{\partial t} = 0$.

证明　由于 f 全纯[3], 于是有

$$f(u(s+h,t)) = f(u(s,t)) + h\frac{\partial u}{\partial s}(s,t) + o(h) = f(u(s,t)) + f'(u(s,t))\left(\frac{\partial u}{\partial t}(s,t)h\right) + o(h).$$

由此得到 (包括对于 $\frac{\partial u}{\partial t}$ 的同样推理)

$$\frac{\partial (f\circ u)}{\partial s} = \frac{\partial u}{\partial s}\cdot f\circ u \quad 和 \quad \frac{\partial (f\circ u)}{\partial t} = \frac{\partial u}{\partial t}\cdot f'\circ u.$$

因为 $P = \frac{\partial u}{\partial s}\cdot f\circ u$ 而 $Q = \frac{\partial u}{\partial t}\cdot f\circ u$, 故有

$$\begin{aligned}-\frac{\partial P}{\partial t} + \frac{\partial Q}{\partial s} &= \frac{\partial^2 u}{\partial t\partial s}\cdot f\circ u - \frac{\partial u}{\partial s}\frac{\partial u}{\partial t}\cdot f'\circ u + \frac{\partial^2 u}{\partial s\partial t}\cdot f\circ u - \frac{\partial u}{\partial t}\frac{\partial u}{\partial s}\cdot f'\circ u \\ &= \left(-\frac{\partial^2 u}{\partial t\partial s} + \frac{\partial^2 u}{\partial s\partial t}\right) f\circ u = 0.\end{aligned}$$

□

定理 VI.1.3. — 设 Ω 是 $\mathbf{C}$ 的一个开集, f 是 Ω 上的一个复 $\mathscr{C}^1$ 类函数. 如果 γ_0, γ_1 是 Ω 中两条同伦的闭道, 则

$$\int_{\gamma_0} f(z)dz = \int_{\gamma_1} f(z)dz.$$

注记 VI.1.4. — 如果 γ 是一条常值闭道, 则对任意的 1-形式 ω 有 $\int_\gamma \omega = 0$. 由此得到, 如果 $\omega = f(z)dz$, 其中 f 在 Ω 上全纯, 则有如下结果: [380]

[3] 一个要求更多知识但更自然的证明在于注意到, 一方面有 $(-\frac{\partial P}{\partial t} + \frac{\partial Q}{\partial s})ds\wedge dt = d(u^*(f(z)dz))$, 另一方面有 $d(u^*(f(z)dz)) = u^*(d(f(z)dz))$, 以及由于 f 全纯而有 $\frac{\partial f}{\partial \bar z} = 0$, 故 $d(f(z)dz) = \frac{\partial f}{\partial \bar z}d\bar z\wedge dz = 0$.

(i) 如果 γ 是在 Ω 中的可缩闭道, 则 $\int_\gamma f(z)dz = 0$.

(ii) 如果 Ω 可缩 (特别地, 如果 Ω 为星形的), 则对 Ω 中任意的闭道有 $\int_\gamma f(z)dz = 0$.

证明　我们先假定在 Ω 上存在在 Ω 中从 γ_0 到 γ_1 的一个 $\mathscr{C}^2$ 类的同伦. 换句话说, 存在一个 $\mathscr{C}^2$ 类的映射 $u:[0,1]^2 \to \Omega$. 使得 $u(0,t) = \gamma_0(t)$ 而 $u(1,t) = \gamma_1(t)$, 并且对所有的 $s \in [0,1]$ 有 $u(s,0) = u(s,1)$. 以 ω 记 1-形式 $f(z)dz$. 将 $u^*\omega$ 写为 $Pds + Qdt$ 的形式. 按照引理 VI.1.2, 有 $-\frac{\partial P}{\partial t} + \frac{\partial Q}{\partial s} = 0$. 因此从命题 VI.1.1 知 $\int_{\partial([0,1]^2)} u^*\omega$ 为 0. 注意 $A = (0,0), B = (1,0), C = (1,1), D = (0,1)$ 是正方形 $[0,1]^2$ 的顶点, 我们便得到

$$\begin{aligned}\int_{[B,C]} u^*\omega = \int_0^1 Q(1,t)dt &= \int_0^1 f(u(1,t))\frac{\partial u}{\partial t}(1,t)dt \\ &= \int_0^1 f(\gamma_1(t))\gamma_1'(t)dt = \int_{\gamma_1} f(z)dz.\end{aligned}$$

同样地, $\int_{[D,A]} u^*\omega = -\int_{\gamma_0} f(z)dz$. 另外, 因为对所有的 $s \in [0,1]$ 有 $u(s,0) = u(s,1)$, 故 $\int_{[A,B]} u^*\omega + \int_{[C,D]} u^*\omega = 0$. 因此得到

$$\begin{aligned}0 = \int_{\partial([0,1]^2)} u^*\omega &= \int_{[A,B]} u^*\omega + \int_{[B,C]} u^*\omega + \int_{[C,D]} u^*\omega + \int_{[D,A]} u^*\omega \\ &= \int_{\gamma_1} f(z)dz - \int_{\gamma_0} f(z)dz,\end{aligned}$$

这便证明了在 γ_0 和 γ_1 在 Ω 中为 $\mathscr{C}^2$ 类同伦的特殊情形下的断言.

转到一般情形. 这时 γ_0 和 γ_1 为分段 $\mathscr{C}^1$ 的道路, 并令 $u:[0,1]^2 \to \Omega$ 为连续映射, 使得 $u(0,t) = \gamma_0, u(1,t) = \gamma_1(t)$ 及对任意的 $s \in [0,1]$ 有 $u(s,0) = u(s,1)$. 我们的想法是用 $\mathscr{C}^2$ 类的函数 u_ε 去逼近 u: 像在习题 IV.3.26 中那样进行正则化 (参见习题 IV.1.7), 然后取极限. 按此想法进行时必须注意让所构造的逼近是闭道同伦的, 并且不能离开 Ω.

以 $[x]$ 记 $x \in \mathbf{R}$ 的整数部分. 定义 $\tilde{u}:[-1,2]^2 \to \Omega$ 为

$$\tilde{u}(s,t) = \begin{cases} u(0, t-[t]), & s \leqslant 0, \\ u(s, t-[t]), & 0 \leqslant s \leqslant 1, \\ u(1, t-[t]), & s \geqslant 1. \end{cases}$$

由构造知 $\tilde{u}$ 连续并在 $[0,1]^2$ 上与 u 重合, 且是一个周期为 1 的 t 的周期函数的限制, 而且它的像与 u 的像重合. 由于 $[-1,2]^2$ 为紧集, 故它在 $\tilde{u}$ 下的像 K 也为紧集, 从而 K 到闭集 $\mathbf{C} - \Omega$ 的距离 $d(K, \mathbf{C}-\Omega) > 0$. 于是存在 $\delta > 0$ 使得 Ω 包含了 $K_\delta = \{z \in \mathbf{C}, d(z,K) \leqslant \delta\}$. 现在如果 $\varepsilon > 0$, 令

$$\delta(\varepsilon) = \sup_{(s',t',s,t)\in[-1,2]^4, |s'-s|\leqslant\varepsilon, |t-t'|\leqslant\varepsilon} |\tilde{u}(s',t') - \tilde{u}(s,t)|.$$

由于 $[-1,2]^2$ 为紧集, 故 $\tilde{u}$ 在 $[-1,2]^2$ 上一致连续, 这等同于当 $\varepsilon \to 0$ 时 $\delta(\varepsilon) \to 0$. 选取 $\varepsilon_0 \leqslant \frac{1}{2}$, 使得当 $\varepsilon \leqslant \varepsilon_0$ 时有 $\delta(\varepsilon) \leqslant \delta$. 最后选取 $\varphi : \mathbf{R} \to \mathbf{R}_+$ 属于 $\mathscr{C}^2$, 并在 $[-1,1]$ 之外为 0, 同时 $\int_{\mathbf{R}} \varphi = 1$, 并定义 $\varphi_\varepsilon(x) = \varepsilon^{-1}\varphi(\varepsilon^{-1}x)$, 这使得 φ_ε 是一个 $\mathbf{R}$ 上的 $\mathscr{C}^2$ 类的正函数, 并且在 $[-\varepsilon, \varepsilon]$ 外为 0, 同时 $\int_{\mathbf{R}} \varphi_\varepsilon = 1$.

以 $\varphi_\varepsilon^{[2]} : \mathbf{R}^2 \to \mathbf{R}$ 记由 $\varphi_\varepsilon^{[2]}(s,t) = \varphi_\varepsilon(s)\varphi_\varepsilon(t)$ 定义的函数. 如果 $\varepsilon \leqslant \varepsilon_0$, 令 u_ε 为 $\tilde{u} * \varphi_\varepsilon^{[2]}$ 在 $[-\frac{1}{2}, \frac{2}{3}]$ 上的限制. 由此有 [381]

$$u_\varepsilon(s,t) = \int_{s-\varepsilon}^{s+\varepsilon} \int_{t-\varepsilon}^{t+\varepsilon} \tilde{u}(x,y)\varphi_\varepsilon(s-x)\varphi_\varepsilon(t-y)dydx,$$

因为当 $x \in [s-\varepsilon, s+\varepsilon]$ 和 $y \in [t-\varepsilon, t+\varepsilon]$ 时有 $|\tilde{u}(x,y) - \tilde{u}(s,t)| \leqslant \delta(\varepsilon)$, 故得到

$$\begin{aligned}|u_\varepsilon(s,t) - \tilde{u}(s,t)| &= |\int_{s-\varepsilon}^{s+\varepsilon} \int_{t-\varepsilon}^{t+\varepsilon} (\tilde{u}(x,y) - \tilde{u}(s,t))\varphi_\varepsilon(s-x)\varphi_\varepsilon(t-y)dydx| \\ &\leqslant \int_{s-\varepsilon}^{s+\varepsilon} \int_{t-\varepsilon}^{t+\varepsilon} |\tilde{u}(x,y) - \tilde{u}(s,t)|\varphi_\varepsilon(s-x)\varphi_\varepsilon(t-y)dydx \\ &\leqslant \int_{s-\varepsilon}^{s+\varepsilon} \int_{t-\varepsilon}^{t+\varepsilon} \delta(\varepsilon)\varphi_\varepsilon(s-x)\varphi_\varepsilon(t-y)dydx = \delta(\varepsilon),\end{aligned}$$

这不但证明了 u_ε 在 $\varepsilon \leqslant \varepsilon_0$ 时取值在 $K_\delta \subset \Omega$ 中还证明了当 ε 趋向 0 时 u_ε 在 $[-\frac{1}{2}, \frac{3}{2}]^2$ 上趋向 u.

另外, 由于 $\varphi_\varepsilon^{[2]}$ 在 $\mathbf{R}^2$ 上属于 $\mathscr{C}^2$ 类并具有紧支集, 故而 $\tilde{u} * \varphi_\varepsilon^{[2]}$ 也如此, 又由于当 $s \in [-1,2]$ 和 $t \in [-2,0]$ 时 $\tilde{u}(s,t+1) = \tilde{u}(s,t)$, 故当 $\varepsilon \leqslant \frac{1}{2}, s \in [-\frac{1}{2}, \frac{3}{2}]$ 以及 $t \in [-\frac{1}{2}, \frac{1}{2}]$ 时有 $u_\varepsilon(s,t+1) = u_\varepsilon(s,t)$. 将其特别应用到 $t=0$, 于是得到, 对于 $s \in [-\frac{1}{2}, \frac{3}{2}]$ 和 $\varepsilon \leqslant \varepsilon_0$, $\gamma_{s,\varepsilon} = u_\varepsilon(s,\cdot)$ 是 Ω 中的一个闭道同伦. 总而言之, 我们已经证明了, 如果 $\varepsilon \leqslant \varepsilon_0$ 那么 u_ε 是 Ω 中一个 $\mathscr{C}^2$ 类的闭道同伦. 由此得到 $\int_{\gamma_{s,\varepsilon}} f(z)dz$ 与 $s \in [-\frac{1}{2}, \frac{3}{2}]$ 无关. 特别对于任意的 $\varepsilon \leqslant \varepsilon_0$ 有

$$\int_{\gamma_{-\frac{1}{2},\varepsilon}} f(z)dz = \int_{\gamma_{\frac{3}{2},\varepsilon}} f(z)dz.$$

然而由构造知, 如果 $s \leqslant 0$, 那么 $\tilde{u}(s,t) = \gamma_0(t)$. 由此推出

$$\begin{aligned}\gamma_{-\frac{1}{2},\varepsilon}(t) &= \int_{-\frac{1}{2}-\varepsilon}^{-\frac{1}{2}+\varepsilon} \int_{t-\varepsilon}^{t+\varepsilon} \gamma_0(t)\varphi_\varepsilon\left(-\frac{1}{2} - x\right)\varphi_\varepsilon(t-y)dxdy \\ &= \int_{t-\varepsilon}^{t+\varepsilon} \gamma_0(t)\varphi_\varepsilon(t-y)dy = (\gamma_0 * \varphi_\varepsilon)(t),\end{aligned}$$

从而 $\gamma'_{-\frac{1}{2},\varepsilon} = \gamma'_0 * \varphi_\varepsilon$. 于是我们已经证明了 $\gamma_{-\frac{1}{2}.\varepsilon}(t) = u_\varepsilon(-\frac{1}{2}, t)$ 趋向 $\tilde{u}(-\frac{1}{2}, t) = \gamma_0(t)$; 同样的推理证明, 当 t 不是 γ_0 的角点时, $\gamma'_{-\frac{1}{2},\varepsilon}(t) \to \gamma'_0(t)$. 最后, 如果 $t \in [0,1]$, 则有

$$|f(\gamma_{-\frac{1}{2},\varepsilon}(t))\gamma'_{-\frac{1}{2},\varepsilon}(t)| \leqslant \sup_{z \in K_\delta} |f(z)| \cdot \sup_{t \in [0,1]} |\gamma'_0(t)|,$$

这让我们从控制收敛定理推出, 当 $\varepsilon \to 0$ 时,

$$\int_{\gamma_{-\frac{1}{2},\varepsilon}} f(z)dz = \int_0^1 f(\gamma_{-\frac{1}{2},\varepsilon}(t))\gamma'_{-\frac{1}{2},\varepsilon}(t)dt \to \int_0^1 f(\gamma_0(t))\gamma'_0(t)dt = \int_{\gamma_0} f(z)dz.$$

同样可证明 $\int_{\gamma_{\frac{3}{2},\varepsilon}} f(z)dz \to \int_{\gamma_1} f(z)dz$, 而取极限的结果是我们得到 $\int_{\gamma_0} f(z)dz = \int_{\gamma_1} f(z)dz$. 这就最终完成了证明. □

3. 柯西公式的第二个证明

仍采用定理 V.4.6 中的记号 (图 1). 如果 $\varepsilon \in]0, r - |z - z_0|[$, 则令

$$u(s,t) = (1-s)(z_0 + re^{2i\pi t}) + s(z + \varepsilon e^{2i\pi t}) = (1-s)z_0 + sz + ((1-s)r + s\varepsilon)e^{2i\pi t}.$$

于是 $\gamma_s(t) = u(s,t)$ 是沿正方向的, 中心为 $c(s) = (1-s)z_0 + sz$, 半径为 $r(s) = (1-s)r + s\varepsilon$ 的圆. 因此有 $\gamma_0 = C(z_0, r)$ 和 $\gamma_1 = C(z, \varepsilon)$. 另外, 对于任意的 $s \in [0,1]$ [382]

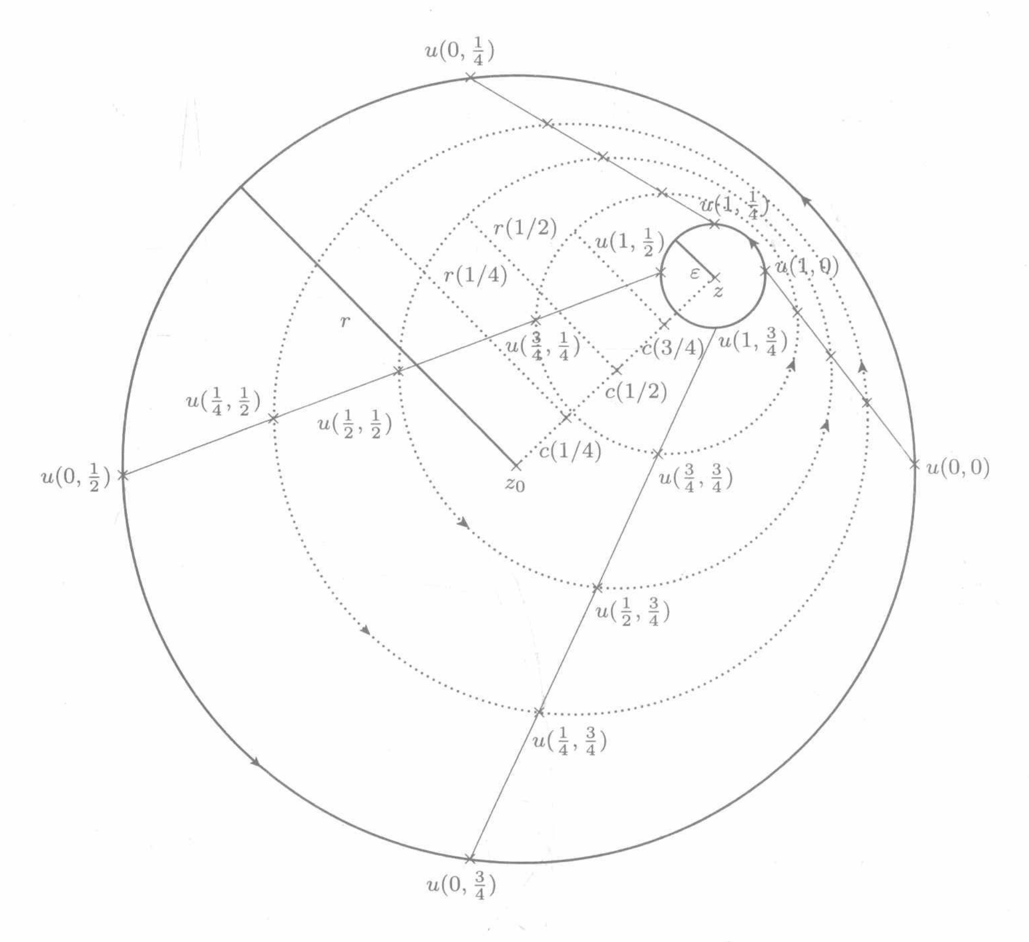


图 1. 从 $C(z_0, r)$ 到 $C(z, \varepsilon)$ 的同伦

有 $u(s,0)=u(s,1)$ 和

$$|u(s,t)-z| \geqslant |r(s)-|c(s)-z|| = s\varepsilon+(1-s)(r-|z-z_0|) \geqslant \varepsilon,$$
$$|u(s,t)-z_0| \leqslant |c(s)-z_0|+r(s) = r-s(r-|z-z_0|-\varepsilon) \leqslant r,$$

这证明了 u 是在 $D(z_0,r)-D(z,\varepsilon^-)\subset\Omega-\{z\}$ 中的一个从 $C(z_0,r)$ 到 $C(z,\varepsilon)$ 上的闭道同伦.

由于 $\frac{f(w)}{w-z}$ 在 $\Omega-\{z\}$ 上 (对于 w) 属于复 $\mathscr{C}^1$ 类, 那么由定理 VI.1.3 得到

$$\frac{1}{2i\pi}\int_{C(z_0,r)}\frac{f(w)}{w-z}dw=\frac{1}{2i\pi}\int_{C(z,\varepsilon)}\frac{f(w)}{w-z}dw,$$

其中 $\varepsilon>0$ 任意. 但 $C(z,\varepsilon)$ 是道路 $t\mapsto z+\varepsilon e^{2i\pi t}$, 从而当 ε 趋向 0 时, $\frac{1}{2i\pi}\int_{C(z,\varepsilon)}\frac{f(w)}{w-z}dw$ $=\int_0^1 f(z+\varepsilon e^{2i\pi t})dt$ 趋向 $\int_0^1 f(z)dt=f(z)$ (依赖一个参数的积分的连续性定理: 由于 f 全纯故在 z 的邻域它对 z 连续). 取极限便得到 $\frac{1}{2i\pi}\int_{C(z_0,r)}\frac{f(w)}{w-z}dw=f(z)$, 这就是我们想要证明的.

VI.2. 一个闭道相对于一个点的指数 [383]

1. 原函数

设 Ω 是 $\mathbf{C}$ 的一个连通开集. 如果 f 在 Ω 上全纯, 称 $F:\Omega\to\mathbf{C}$ 是 f 的一个*原函数*是说, F 在 Ω 上全纯且 $F'=f$. 如果 $\gamma:[a,b]\to\Omega$ 是一条 $\mathscr{C}^1$ 类道路, 则 $(F\circ\gamma)'(t)=f(\gamma(t))\gamma'(t)$, $t\in[a,b]$ 任意.

一个全纯函数总具有*局部的*原函数, 事实上, 如果 f 在 $D(z_0,r^-)$ 中全纯, 则根据注记 V.4.9 的 (i), 有 $f(z)=\sum_{n=0}^{+\infty}\frac{f^{(n)}(z_0)}{n!}(z-z_0)^n$, 从而 f 具有在 $D(z_0,r^-)$ 上的原函数 F, 其定义为 $F(z)=\sum_{n=0}^{+\infty}\frac{f^{(n)}(z_0)}{(n+1)!}(z-z_0)^{n+1}$. 另一方面, 在任意的一个开集 Ω 上并不总具有在整个 Ω 上的原函数.

命题 VI.2.1. — *设 Ω 是 $\mathbf{C}$ 的一个连通开集. 如果 f 在 Ω 上全纯, 则以下条件等价:*

(i) f 在 Ω 上具有原函数 F;

(ii) 对所有包含在 Ω 中的分段 $\mathscr{C}^1$ 类的闭道 γ 有 $\int_\gamma f(z)dz=0$.

证明 如果 f 在 Ω 上有一个原函数 F, 则 $f(z)dz=dF$. 应用定理 V.4.2 的 (iv) 得到 $\int_\gamma f(z)dz=F(\gamma(b))-F(\gamma(a))$, 其中 $\gamma:[a,b]\to\Omega$ 属于 $\mathscr{C}^1$ 类. 特别地, 如果 γ 是条闭道, 则因 $\gamma(b)=\gamma(a)$ 有 $\int_\gamma f(z)dz=0$. 故得 (i)⇒(ii). 转而证明相反的方向. 固定 $a\in\Omega$. 如果 γ_1 和 γ_2 是 Ω 中端点为 a 和 b 的分段 $\mathscr{C}^1$ 的两条道路 [4], 从而得到由 γ_1 与反向的 γ_2 连接的闭道 γ; 因此由假设条件有 $\int_{\gamma_1}f(z)dz-\int_{\gamma_2}f(z)dz=\int_\gamma f(z)dz=0$.

[4] 由 $\mathbf{R}^n$ 的一个连通开集是道路连通的证明可推出一个这样的开集也是折线连通的 (有限条线段的并), 从而也就是分段 $\mathscr{C}^1$ 类道路连通的.

这让我们可以定义函数 $F:\Omega\to\mathbf{C}$ 为 $F(b)=\int_\gamma f(z)dz$, 其中 γ 是任意一条 Ω 中的分段 $\mathscr{C}^1$ 的道路, 其端点为 a 和 b.

只要证明 F 复可导, 且对 Ω 中的任意点 z_0 的导数为 $f(z_0)$ 即可: 由命题 V.4.7 可证明 F 是全纯的. 那么, 设 $z_0\in\Omega$ 及 $r>0$, 使得 $D(z_0,r^-)\subset\Omega$. 如果固定一条在 Ω 中连接 a 到 z_0 的道路 γ_0, 且若 $b\in D(z_0,r^-)$, 我们作一条连接 a 到 b 的 Ω 中道路 γ_b, 并将线段 $[z_0,b]$ 连接道路 γ_0. 于是有

$$\frac{F(b)-F(z_0)}{b-z_0}=\frac{1}{b-z_0}\left(\int_{\gamma_0}f(z)dz+\int_{[z_0,b]}f(z)dz-F(z_0)\right)=\int_0^1 f(z_0+t(b-z_0))dt,$$

而 f 在 z_0 的连续性证明了 (例如, 利用依赖一个参数的积分的连续性), 当 $b\to z_0$ 时有 $\frac{F(b)-F(z_0)}{b-z_0}\to f(z_0)$. 得到所要结果. □

[384] **注记 VI.2.2.** — (i) 根据注记 VI.1.4 的 (ii), 当 Ω 是一个星形开集, 或更一般地可缩时, 条件 (ii) 自动满足. 由此得到在一个可缩开集上的全纯函数总有原函数.

(ii) 如果 $a\in\mathbf{C}$, 且 $a<R_1<R_2$, 则函数 $\frac{1}{z-a}$ 在圆环 $C(a,R_1,R_2)$ 上全纯, 但如果 $R_1<r<R_2$, 则 $\int_{C(a,r)}\frac{dz}{z-a}=2i\pi\neq 0$. 函数 $\frac{1}{z-a}$ 因而在圆环 $C(a,R_1,R_2)$ 上没有原函数而这个圆环也不是可缩的.

命题 VI.2.3. — (全纯函数的对数)

设 Ω 是 $\mathbf{C}$ 的一个可缩开集, 且 f 在 Ω 上全纯而且在 Ω 上不取 0. 于是存在 Ω 上的全纯函数 g, 使得 $f=e^g$, 从而有 $g'=\frac{f'}{f}$.

证明　由于 Ω 可缩, 且因为 $\frac{f'}{f}$ 在 Ω 上全纯, 故根据注记 VI.2.2 的 (i) 存在 Ω 上的全纯函数 h 使得 $h'=\frac{f'}{f}$. 设 $z_0\in\Omega$, 必要时对 h 添加常数, 故可设 $e^{h(z_0)}=f(z_0)$. 从而有 $(e^{-h}f)'=-h'e^{-h}f+e^{-h}f'=0$, 因此 $e^{-h}f$ 在 Ω 上为常数, 又由于它在 z_0 取值为 1, 故在 Ω 上 $f=e^h$. 如果 g 是另一个 Ω 上满足 $e^g=f$ 的全纯函数, 则有 $e^{g-h}=1$, 从而 $g-h$ 全纯并在 $2i\pi\mathbf{Z}$ 中取值. 因为 Ω 连通, $g-h$ 为常数从而 $g'=\frac{f'}{f}$. □

习题 VI.2.4. — (莫雷拉 (Morera) 定理) 设 $z_0\in\mathbf{C}$, $r>0$.

(i) 证明, 如果 f 在 $D(z_0,r^-)$ 上全纯, 则对任意的 $a,b,c\in D(z_0,r^-)$ 有

$$\int_{[a,b]}f(z)dz+\int_{[b,c]}f(z)dz+\int_{[c,a]}f(z)dz=0. \qquad \text{(VI.2.1)}$$

(ii) 设 $f:D(z_0,r^-)\to\mathbf{C}$ 连续且满足性质 (VI.2.1). 令 $F(z)=\int_{[z_0,z]}f(z)dz$. 证明 $\frac{1}{h}(F(z+h)-F(z))$ 当 h 趋向 0 时趋向 $f(z)$. 由此推出 F 和 f 全纯.

(iii) 设 Ω 为 $\mathbf{C}$ 的一个开集. 证明 $f:\Omega\to\mathbf{C}$ 全纯当且仅当 f 连续并且对任意的 $a,b,c\in\Omega$ 有 $\int_{[a,b]}f(z)dz+\int_{[b,c]}f(z)dz+\int_{[c,a]}f(z)dz=0$, 其中以 a,b,c 为顶点的三角形全部 (即连同其内核) 包含在 Ω 中.

2. 绕一个点的闭道的圈数

设 $z_0 \in \mathbf{C}$, 而 γ 是一条不通过 z_0 的闭道. 这里我们的目的是从数学上定义 γ 绕 z_0 的圈数.

2.1. 定义

引理 VI.2.5. — 设 $\gamma : [a,b] \to \mathbf{C} - \{z_0\}$ 为一条分段 $\mathscr{C}^1$ 的道路. 如果 $t \in [a,b]$, 令 γ_t 为 γ 在 $[a,t]$ 上的限制, 而 $f(t) = \int_{\gamma_t} \frac{dz}{z-z_0}$. 于是 $e^{-f(t)}(\gamma(t) - z_0)$ 在 $[a,b]$ 上为常数.

证明 按定义有 $f(t) = \int_0^t \frac{\gamma'(u)}{\gamma(u)-z_0}du$, 从而对于 t 不是 γ 的角点时有 $f'(t) = \frac{\gamma'(t)}{\gamma(t)-z_0}$. 因此 $t \mapsto e^{-f(t)}(\gamma(t) - z_0)$ 的导数为 [385]

$$-f'(t)e^{-f(t)}(\gamma(t) - z_0) + e^{-f(t)}\gamma'(t) = e^{-f(t)}(-\frac{\gamma'(t)}{\gamma(t) - z_0}(\gamma(t) - z_0) + \gamma'(t)) = 0,$$

因此 g 为分段常值的; 又由于它连续故得结论. □

推论 VI.2.6. — 如果 $\gamma : [a,b] \to \mathbf{C}$ 是一条不通过 z_0 的分段 $\mathscr{C}^1$ 的闭道, 则 $I(\gamma, z_0) = \frac{1}{2i\pi}\int_\gamma \frac{dz}{z-z_0}$ 是一个整数.

证明 沿用上面引理的记号, 我们看到 $e^{f(b)} = e^{f(a)}\frac{\gamma(b)-z_0}{\gamma(a)-z_0}$, 并且由于 γ 是一个闭道, 故 $\exp(\int_\gamma \frac{dz}{z-z_0}) = e^{f(b)} = e^{f(a)} = 1$, 便得到结论. □

上面所定义的 $I(\gamma, z_0)$ 是 γ 对于 z_0 的指标. 例如, 一方面如果 γ 是道路 $C(a,r)$, 而 $|z_0 - a| < r$, 那么对常值函数 1 应用柯西公式便证明了 $I(C(a,r), z_0) = 1$. 另一方面, 如果 $|z_0 - a| > r$, 则圆 $C(z_0, r)$ 在 $\mathbf{C} - \{z_0\}$ 中同伦于 $\{a\}$, 而因为 $\frac{1}{z-z_0}$ 在 $\mathbf{C} - \{z_0\}$ 中全纯, 故 $I(C(a,r), z_0) = 0$. 换句话说, 当 z_0 在正向圆的内部时, 该圆对于 z_0 的指标为 1, 而当 z_0 在其外部时, 指标为 0. 这与沿 γ 时 $I(\gamma, z_0)$ 代表了 γ 绕 z_0 的次数的想法一致. 我们应注意, 如果此圆沿相反的方向进行, 它对于内部一点的指标则为 -1.

2.2. 直观地确定闭道对于一个点的指标

在本书考虑的情形中, 这些闭道是没有二重点的 (并由线段和圆弧构成), 而若尔当的一个定理断言, 这样的一条闭道将平面分割成两个区域, 一个是闭道的内部, 另一个是它的外部, 我们发现像圆一样的图形便是这种情形. 在一般的情形, 确定在一个图形上一条闭道对于一条道路的指标可能教人头昏脑胀, 但后面的命题 VI.2.7 给出了一个可直接计算的方法.

方法如下. 选择一个足够大的点 $a \in \mathbf{C}$ 使得 $\gamma \subset D(0, |a|^-)$, 并作一条从 a 到 z_0 的道路 u. 于是 $I(\gamma, z_0) = n_g - n_d$, 其中 n_g(分别地, n_d)[5] 是当我们从 a 走到 z_0 时 u 与 γ 的从左边 (分别地, 从右边) 穿过的相交点的个数 (图 2).

[5] 要使这样做有意义, 应该加以小心: 譬如, 要求 u 与 γ 只交于 γ 的非角点的简单点, 而在交点的 γ 的切线与 u 的切线不共线.

事实上, 设 γ 是 $\mathbf{C}$ 的一条闭道. 由于 γ 为紧集 (作为紧区间在连续映射下的像), 它的补集为开集, 而此补集的每个连通分支为开集. 另外, 如果 R 充分大, γ 便包含在 $D(0,R)$ 中, 又因为 $\mathbf{C}-D(0,R)$ 连通, 于是当 R 充分大时, 有 $\mathbf{C}-\gamma$ 的一个且唯一的连通分支包含了 $\mathbf{C}-D(0,R)$. 称这个连通分支为*无限远连通分支*.

[386]

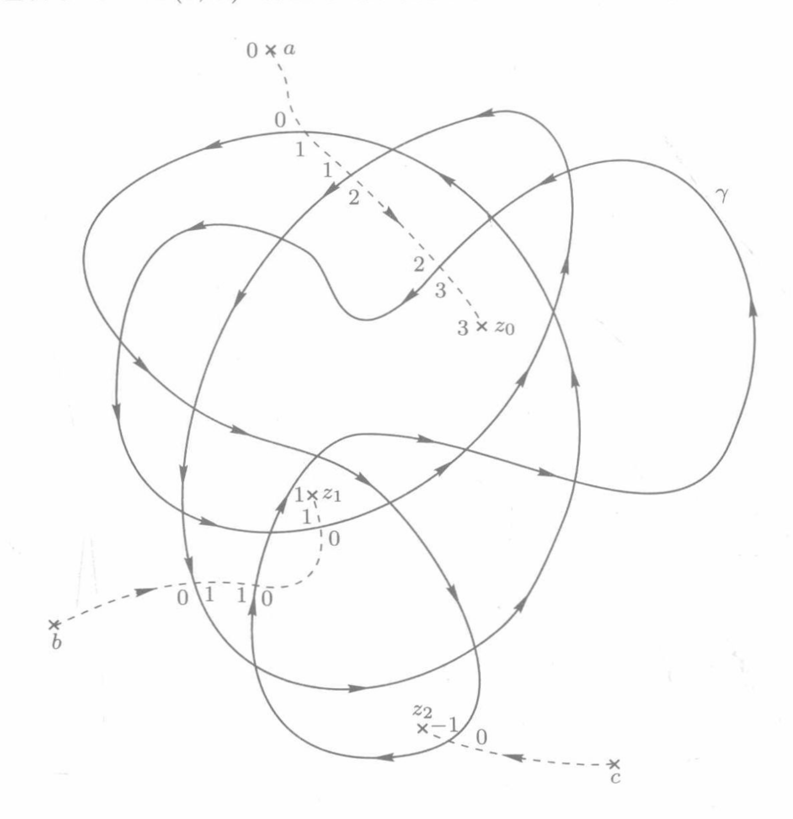


图 2. $I(\gamma,z_0)=3 \quad I(\gamma,z_1)=1, \quad I(\gamma,z_2)=-1$

命题 VI.2.7. — *设 γ 为分段 $\mathscr{C}^1$ 的闭道.*

(i) $z\mapsto I(\gamma,z)$ 在 $\mathbf{C}-\gamma$ 的每一个连通分支上为常数.

(ii) 如果 z 在 $\mathbf{C}-\gamma$ 的无限远连通分支, 则 $I(\gamma,z)=0$.

(iii) 设 $t\mapsto\gamma(t), t\in[a,b]$ 是 γ 的参数化, 其为分段 $\mathscr{C}^1$, 并且 $t_0\in[a,b]$ 使得 $\gamma(t_0)$ 是 γ 的一个简单点, 而且 $\gamma'(t_0)\neq 0$. 如果 $h\in\mathbf{C}$ 满足 $\mathrm{Im}(h)>0$, 并设 $\varepsilon>0$ 充分小, 于是

- *$\gamma(t_0)+\varepsilon h\gamma'(t_0)$ 和 $\gamma(t_0)-\varepsilon h\gamma'(t_0)$ 不属于 γ,*
- *$I(\gamma,\gamma(t_0)+\varepsilon h\gamma'(t_0))-I(\gamma,\gamma(t_0)-\varepsilon h\gamma'(t_0))=1$.*

证明 利用依赖一个参数的积分的连续性定理可以证明 $z_0\mapsto I(\gamma,z_0)$ 在 $\mathbf{C}-\gamma$ 上的连续性, 并由于 $I(\gamma,z_0)$ 在 $\mathbf{Z}$ 中取值, 而 $\mathbf{Z}$ 离散, 故这证明了 (i).

如果 $\gamma\subset D(0,R)$, 且 $|z_0|>R$, 则 γ 在 $\mathbf{C}-\{z_0\}$ 中同伦于一个点 (由于 $D(0,R)$

可缩, 同样在 $D(0,R)$ 中同伦于一个点), 又由于 $\frac{1}{z-z_0}$ 在 $\mathbf{C}-\{z_0\}$ 中全纯, 故有 $\int_\gamma \frac{dz}{z-z_0}=0$. 因此对于 $|z_0|>R$ 得到了 (ii), 并由于 (i) 则完成了 (ii) 的证明.

转而证明 (iii). 选取 $h\in\mathbf{C}, \operatorname{Im}(h)>0$. 因此 $0<\arg(h)<\pi$. 如有必要可做变量的平移从而可假设 $t_0=0$, 并必要时用一个相似变换 $z\mapsto\gamma'(t_0)^{-1}(z-\gamma(t_0))$, 从而可设 $\gamma(t_0)=0$ 及 $\gamma'(t_0)=1$, 这样, 这些公式得到一点简化. 于是有 $\lim_{t\to 0} t^{-1}\gamma(t)=1$, 这表明存在 $\delta>0$ 使得对任意的 $t\in[-\delta,\delta]-\{0\}$ 有

- $|\arg(t^{-1}\gamma(t))|<\frac{1}{2}\inf(\arg(h),\pi-(\arg(h))$, [387]
- $|t^{-1}\gamma(t)-1|\leqslant\frac{1}{2}$.

另外, 由于 $0=\gamma(0)$ 是 γ 的一个简单点, 故存在 $\eta>0$ 使得当 $t\in[a,b]-]-\delta,\delta[$ 时有 $d(0,\gamma(t))\geqslant\eta$. 由此我们推出, 如果 $0<\varepsilon<|h|^{-1}\eta$, 则又, $\pm\varepsilon h$ 对于 $t\in[-\delta,\delta]$, 不再具有 $\gamma(t)$ 的形式: 因为当 $t\in[-\delta,\delta]-\{0\}$ 时和 δ 的选取, 故有 $\pm\varepsilon h\neq 0$ 和 $\arg(\frac{\pm\varepsilon h}{\gamma(t)})\neq 0$. 总之, 如果 $0<\varepsilon<|h|^{-1}\eta$, 则 $\pm\varepsilon h$ 不属于 γ.

现在我们有 $I(\gamma,\varepsilon h)-I(\gamma,-\varepsilon h)=I_1(\varepsilon)+I_2(\varepsilon)$, 其中我们令

$$I_1(\varepsilon)=\frac{1}{2i\pi}\int_{\gamma([a,-\delta])\cup\gamma([\delta,b])}\frac{dz}{z-\varepsilon h}-\frac{dz}{z+\varepsilon h}$$

和

$$I_2(\varepsilon)=\frac{1}{2i\pi}\int_{\gamma([-\delta,\delta])}\frac{dz}{z-\varepsilon h}-\frac{dz}{z+\varepsilon h}.$$

由于当 $\frac{1}{z-\varepsilon h}-\frac{1}{z+\varepsilon h}$ 在 $\varepsilon\to 0^+$ 时趋向 0 并且被强函数 $\frac{2}{\eta-\varepsilon|h|}$ 控制, 故 $\lim_{\varepsilon\to 0^+} I_1(\varepsilon)=0$. 因为 $I(\gamma,\varepsilon h)-I(\gamma,-\varepsilon h)\in\mathbf{Z}$, 故要证明对于充分小的 $\varepsilon>0$ 时有 $I(\gamma,\varepsilon h)-I(\gamma,-\varepsilon h)=1$ 只则要证明 $\lim_{\varepsilon\to 0^+} I_2(\varepsilon)=1$ 即可. 为此将 $2i\pi I_2(\varepsilon)$ 写成下面的形式

$$2i\pi I_2(\varepsilon)=\int_{\gamma([-\delta.\delta])}\frac{2\varepsilon h}{z^2-\varepsilon^2h^2}dz=\int_{-\delta}^{\delta}\frac{2\varepsilon h\gamma'(t)}{\gamma(t)^2-\varepsilon^2h^2}dt=\int_{-\delta/\varepsilon}^{\delta/\varepsilon}\frac{2h\gamma'(\varepsilon t)}{\varepsilon^{-2}\gamma(\varepsilon t)^2-h^2}dt.$$

积分号内的表达式当 ε 趋向 0 且 $t\in\mathbf{R}$ 时趋向 $\frac{2h}{t^2-h^2}$. 另外, 由于 δ 的选取, 故存在 $c>0$ 使得当 $u\in[-\delta,\delta]$ 时有 $2\pi-c>\arg(h^2\gamma(u)^{-2})>c$; 由此得知, 存在 $C>0$ (当 $\cos c\leqslant 0$ 时 $C=1$, 而当 $\cos c\geqslant 0$ 时 $C=|\sin c|$) 使得对于任意的 $\mu,\lambda\in\mathbf{R}_+$ 有 $|\lambda\gamma(t)^2-\mu h^2|\geqslant C\sup(|\lambda\gamma(t)^2|,|\mu h^2|)$. 因为 $|\gamma(u)|\geqslant\frac{1}{2}|u|$, 并因为当 $u\in[-\delta,\delta]$ 时, 存在 $M\geqslant 0$ 使得 $|\gamma'(u)|\leqslant M$, 故按模, 在 $[-\delta/\varepsilon,\delta/\varepsilon]$ 上, $\frac{2h\gamma'(\varepsilon h)}{\varepsilon^{-2}\gamma(\varepsilon t)^2-h^2}$ 被 $\frac{2|h|M}{C\sup(t^2/4.|h|^2)}$ 所控制, 而后者是 $\mathbf{R}$ 上的可和函数, 并与 ε 无关. 因此利用依赖一个参数的积分的连续性定理得到

$$\lim_{\varepsilon\to 0^+} 2i\pi I_2(\varepsilon)=\int_{-\infty}^{+\infty}\frac{2h}{t^2-h^2}dt.$$

最后, 令 $h=\sigma+i\tau$, 按假定, $\tau>0$. 那么上面最后的那个积分成为

$$\int_{-\infty}^{+\infty}\frac{dt}{t-h}-\frac{dt}{t+h}=\int_{-\infty}^{+\infty}\frac{(t-\sigma)+i\tau}{(t-\sigma)^2+\tau^2}-\frac{(t+\sigma)-i\tau}{(t+\sigma)^2+\tau^2}dt$$

$$=\left[\frac{1}{2}\log\frac{(t-\sigma)^2+\tau^2}{(t+\sigma)^2+\tau^2}\right]_{-\infty}^{+\infty}+i\left[\arctan\frac{t-\sigma}{\tau}+\arctan\frac{t+\sigma}{\tau}\right]_{-\infty}^{+\infty}=2i\pi,$$

从而得到结论. (注意到在 0 的邻域中, γ 是一个函数的图像, 我们则可给出 (习题)$I_2(\varepsilon)\to 1$ 的一个证明: 这时可以将 $2i\pi I_2(\varepsilon)$ 写为 $\frac{dz}{z}$ 在一条路径 C_ε 上的积分, 这条路径类似于顶点在 $\pm\delta\pm\varepsilon h$ 的但去掉竖直边 (它们的长趋向 0) 的平行四边形. 利用留数公式 (定理 VI.3.13) 可证明, 在 C_ε 上的积分等于 $2i\pi$. 这样我们便可避免上面的强函数了.) □

VI.3. 柯西的留数公式

1. 在圆环上的全纯函数

如果 $z_0\in\mathbf{C}$ 而 $0\leqslant R_1<R_2$, 以 $C(z_0,R_1,R_2)$ 记满足 $R_1<|z-z_0|<R_2$ 的 $z\in\mathbf{C}$ 的开圆环. 如果 $R_1=0$, 则得到中心为 z_0 半径为 R_2 的有孔开圆盘 (即 $D(z_0,R_2^-)-\{z_0\}$).

[388] **引理 VI.3.1.** — *如果 f 是圆环 $C(z_0,R_1,R_2)$ 上的全纯函数, 而 $z\in C(z_0,R_1,R_2)$, 并且 $R_1<r_1<|z-z_0|<r_2<R_2$, 则*

$$f(z)=\frac{1}{2i\pi}\int_{C(z_0,r_2)}\frac{f(w)}{w-z}dw-\frac{1}{2i\pi}\int_{C(z_0,r_1)}\frac{f(w)}{w-z}dw.$$

证明 请读者跟随着按图 3 进行的推理[(6)].

设 $r<\inf(r_2-|z-z_0|,|z-z_0|-r_1)$ 使得 $D(z,r)\subset C(z_0,r_1,r_2)$. 而 $R\in]|z-z_0|-r,|z-z_0|+r[$ 使得圆 $C(z_0,R)$ 和 $C(z,r)$ 交于 a,b 两点. 设 r_0 是 $C(z_0,r)$ 的在 $D(z,r)$ 沿正方向的圆弧. 如有必要交换 a 和 b, 故不妨设这是一条从 b 走到 a 的道路. 令 γ_1'(分别地, γ_2') 是在 $D(z_0,R)$ 内部 (分别地, 外部) 的 $C(z,r)$ 沿反方向 (分别地, 正方向) 的圆弧; 这是一条从 a 到 b 的道路. 如果 $i\in\{1,2\}$, 令 γ_i 为在 $C(z_0,r_1,r_2)-\{2\}$ 中由连接 γ_0 和 γ_i' 得到的闭道; 它们是在 $C(z_0,R_1,R_2)-\{z\}$ 中同

[389] 伦于 $C(z_0,r_i)$ 的闭道[(7)]. 因此有

---

(6)也可以利用斯托克斯公式的推广形式直接得到 $\int_{C(z_0,r_i)}\frac{f(w)}{w-z}dw=\int_{\gamma_i}\frac{f(w)}{w-z}dw$: 因为 f 在由 $C(z_0,r_i)$ 和 γ_i 围成的开集上全纯.

(7)在图 3 中这是完全显见的, 但也可写出一个显式的同伦公式. 例如, 对于从 γ_2 走向 $C(z_0,r_2)$, 我们用 $\gamma_0(t)=z_0+Re^{2i\pi(t-\beta)}$ 对 γ_0 参数化, 其中的 β 选取为使 $\gamma_0(t)=b$, 而 $t\in[0,\alpha]$, 其中 $\alpha<1$ 满足 $\gamma_0(\alpha)=a$, 然后再参数化 γ_2': $\gamma_2'(t)=z+re^{2i\pi(\lambda t+\mu)}$, 其中 $t\in[\alpha,1]$, 这便给出了一个 γ_2 的参数化 $t\mapsto\gamma_2(t),t\in[0,1]$. 最后, 以 $t\mapsto\delta(t)=z_0+r_2e^{2i\pi(t-\beta)},t\in[0,1]$ 对 $C(z_0,r_2)$ 参数化, 从而建立了一个从 γ_2 到 $C(z_0,r_2)$ 的同伦 $u(s,t)$: $u(s,t)=(1-s)\gamma_2(t)+s\delta(t)$. 还需验证这个同伦在 $C(z_0,R_1,R_2)-\{z\}$ 中, 这在图 3 中是显见的 (当 $\gamma_2(t)-z_0$ 和 $\delta(t)-z_0$ 间夹角较小时这可做到, 而当 s 从 0 变到 1 时, $u(s,t)$ 便跑过线段 $[\gamma_2(t),\delta(t)]$).

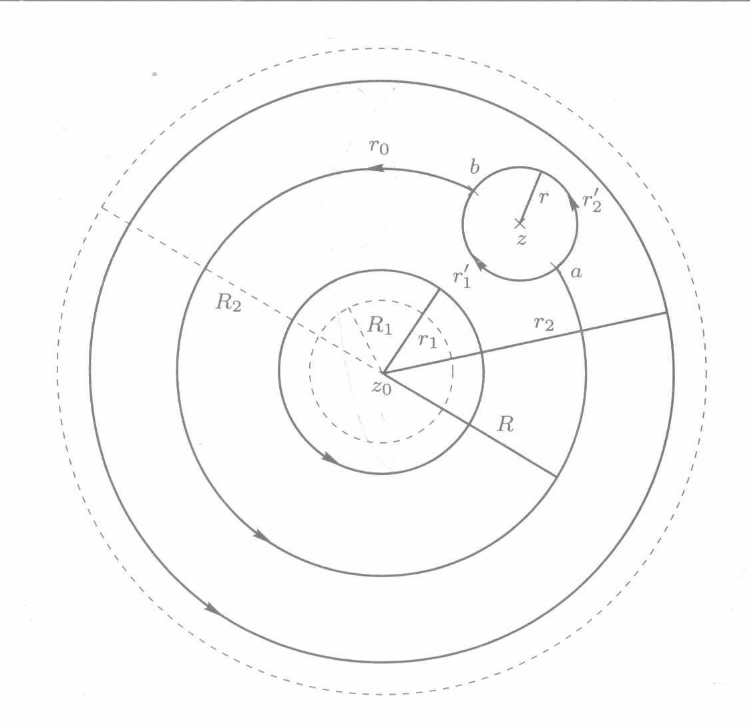


图 3. 用来证明引理的图

$$\begin{aligned}\int_{C(z_0,r_2)}\frac{f(w)}{w-z}dw-\int_{C(z_0,r_1)}\frac{f(w)}{w-z}dw&=\int_{\gamma_2}\frac{f(w)}{w-z}dw-\int_{\gamma_1}\frac{f(w)}{w-z}dw\\&=\int_{\gamma_2'}\frac{f(w)}{w-z}dw-\int_{\gamma_1'}\frac{f(w)}{w-z}dw\\&=\int_{C(z,r)}\frac{f(w)}{w-z}dw\end{aligned}$$

对在 $D(z,r)$ 上全纯的 f 用柯西积分公式便得结果. □

推论 VI.3.2. — 如果 f 在 $C(z_0,R_1,R_2)$ 上全纯, 则存在 $\mathbf{C}$ 中的唯一序列 $(a_n)_{n\in\mathbf{N}}$ 满足

(i) $\sum_{n=0}^{+\infty}a_nz^n$ 当 $|z|<R_2$ 时收敛, 而 $\sum_{n=-\infty}^{-1}a_nz^n$ 当 $|z|^{-1}<R_1^{-1}$ 时收敛; [390]

(ii) 如果 $z\in C(z_0,R_1,R_2)$, 则 $f(z)$ 是 (洛朗) 级数 $\sum_{n\in\mathbf{Z}}a_n(z-z_0)^n$ 的和.

另外, 对于任意的 $r\in]R_1,R_2[$ 和 $n\in\mathbf{N}$ 有

$$a_n=\frac{1}{2i\pi}\int_{C(z_0,r)}(w-z_0)^{-n-1}f(w)dw.$$

证明 如果 $r,r'\in]R_1,R_2[$, 圆 $C(z_0,r)$ 和 $C(z_0,r')$ 在 $C(z_0,R_1,R_2)$ 中同伦. 由于 $(z-z_0)^{-n-1}f(z)$ 在 $C(z_0,R_1,R_2)$ 中全纯, 这让我们能证明 $\frac{1}{2i\pi}\int_{C(z_0,r)}(z-z_0)^{-n-1}d(z)dz$ 不依赖 $r\in]R_1,R_2[$ 的选取; 记其为 a_n. 现在, 根据引理 VI.3.1 (图 4), 如果 $R_1<r_1<$

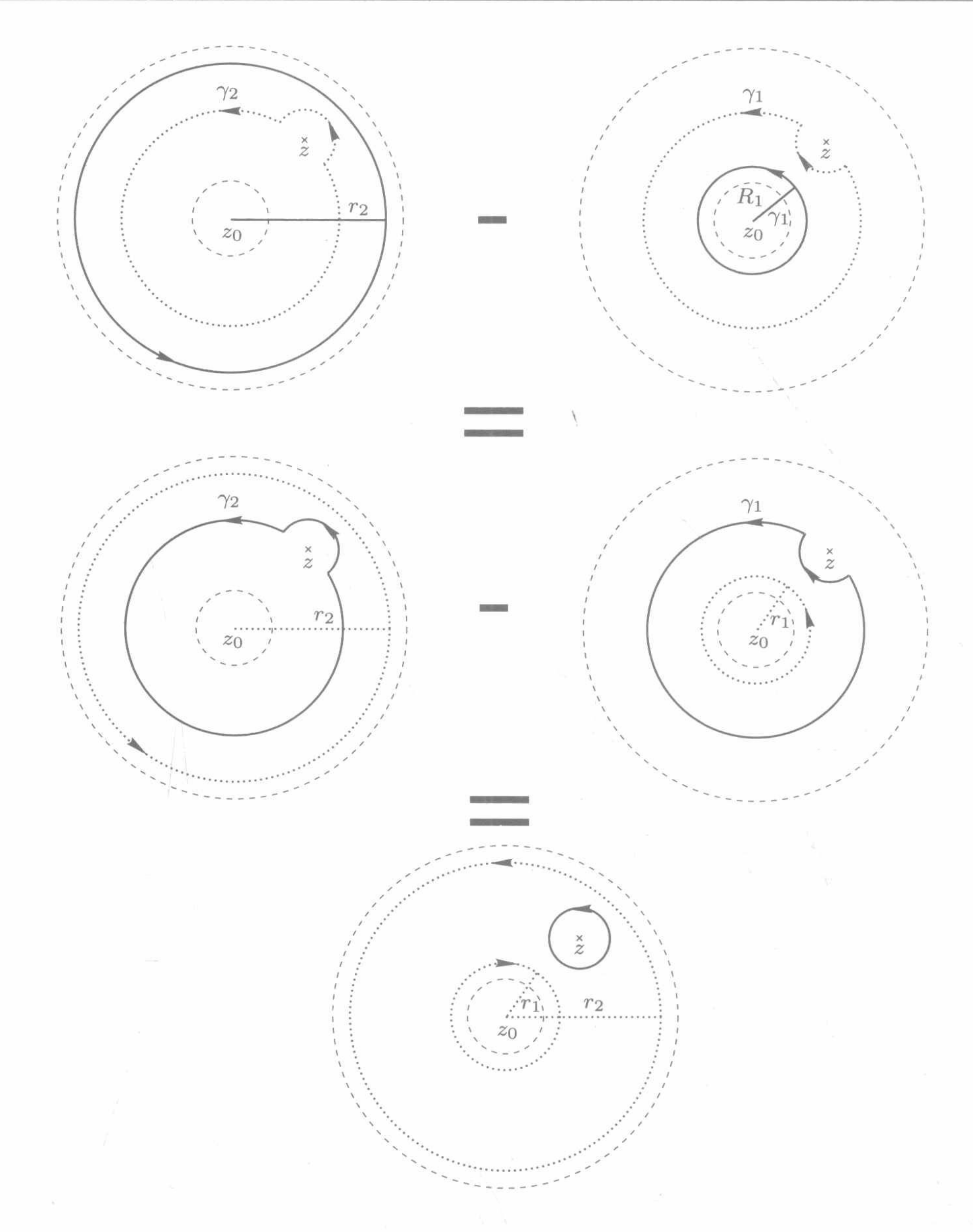


图 4. 用来证明引理 VI.3.1 的图

$|z - z_0| < r_2 < R_2$, 则有

$$f(z) = \frac{1}{2i\pi} \int_{(z_0,r_2)} \frac{f(w)}{w-z} dw - \frac{1}{2i\pi} \int_{C(z_0,r_1)} \frac{f(w)}{w-z} dw.$$

另外,

$$\frac{1}{w-z}=\begin{cases}\displaystyle\sum_{n=0}^{+\infty}\frac{(z-z_0)^n}{(w-z_0)^{n+1}}, & \text{如果}\quad |w-z_0|=r_2,\\ \displaystyle-\sum_{n=0}^{+\infty}\frac{(w-z_0)^n}{(z-z_0)^{n+1}}=-\sum_{n=-\infty}^{-1}\frac{(z-z_0)^n}{(w-z_0)^{n+1}}, & \text{如果}\quad |w-z_0|=r_1.\end{cases}$$

由此, 像在命题 V.4.7 的证明中那样将上述展开式代入积分中便得到了级数 $\sum_{n\in\mathbf{Z}}a_n(z-z_0)^n$ 在圆环 $r_1<|z-z_0|<r_2$ 中按范数收敛 (对于一致范数) 于 $f(2)$. 让 r_1 趋向 R_1, r_2 趋向 R_2 便得结果. □

习题 VI.3.3. — 设 f 在 $\mathbf{C}^*$ 中全纯. 证明存在 $\mathbf{C}$ 中序列 $(a_n)_{n\in\mathbf{Z}}$ 使得对所有 $z\in\mathbf{C}^*$ 有 $f(z)=\sum_{n\in\mathbf{Z}}a_nz^n$.

习题 VI.3.4. — 设 $\mathscr{H}=\{z\in\mathbf{C},\mathrm{Im}(z)>0\}$ 为庞加莱半平面, 而 $f:\mathscr{H}\to\mathbf{C}$ 是一个周期为 1 的全纯周期函数.

(i) 证明存在 $\tilde{f}:D(0,1^-)-\{0\}\to\mathbf{C}$ 的全纯函数使得 $f(z)=\tilde{f}(e^{2i\pi z})$.

(ii) 由此推出, 存在 $a_n(f)\in\mathbf{C},n\in\mathbf{Z}$ 使得 $f(z)=\sum_{n\in\mathbf{Z}}a_n(f)e^{2i\pi nz}$, 其中 $z\in\mathscr{H}$ 任意, 并且此级数在所有水平带 $a\leqslant Im(z)\leqslant b, 0<a<b<+\infty$ 上按范数收敛.

(iii) 证明对所有的 $T>0$ 有 $a_n(f)=\int_{[iT,1+iT]}e^{-2i\pi z}f(z)dz$ (可利用习题 V.4.5).

2. 在有孔圆盘上的全纯函数; 留数

设 Ω 是 $\mathbf{C}$ 的一个开集, $z_0\in\Omega$, 而 f 在 $\Omega-\{z_0\}$ 上全纯, 设 $r>0$ 使得 $D(z_0,r^-)\subset\Omega$. 函数 f 因而在有孔圆盘 $D(z_0,r^-)-\{z_0\}$ 上全纯, 我们也可将有孔圆盘看作为圆环 $C(z_0,0,r)$. 因此可将 1 小节的结果用于它, 从而得到存在一个复数序列 $(a_n)_{n\in\mathbf{Z}}$ 满足如下条件:

- 级数 $g(z)=\sum_{n=0}^{+\infty}a_n(z-z_0)^n$ 在 $D(z_0,r^-)$ 中收敛;
- 级数 $h(z)=\sum_{n\leqslant-1}a_n(z-z_0)^n$ 在 $\mathbf{C}-\{z_0\}$ 中收敛并定义了一个全纯函数;
- 对任意的 $z\in D(z_0,r^-)-\{z_0\}$, $f(z)=\sum_{n\in\mathbf{Z}}a_n(z-z_0)^n$.

称级数 $h(z)$ 为 f 在 z_0 的奇异部分, 而 $(z-z_0)^{-1}$ 的系数 a_{-1} 是 f 在 z_0 的留数, 记为 $\mathrm{Res}(f,z_0)$. f 在 z_0 全纯[8] 是指 $h=0$. 更一般地, 称 f 在 z_0 为亚纯的是说存在 $k\in\mathbf{Z}$ 使得当 $n\leqslant k$ 时 $a_n=0$. 如果 $k\geqslant1$ 为一个整数, 那么称 f 在 z_0 有一个 k 阶极点是指 $a_{-k}\neq0$ 而对所有的 $n<-k$ 有 $a_n=0$[9]. 称 f 在 z_0 有一个本性奇点是说它在 z_0 不是亚纯的. [391]

---

[8] 这有滥用术语之嫌, 但这里想要说的是, 函数 f 可以连续地延拓到 z_0, 而这样得到的函数在 $D(z_0,r^-)$ 上全纯.

[9] 因此 f 在 z_0 为亚纯函数当且仅当它为全纯函数或者有一个有限阶的极点.

我们可以用以下定义的 f 的赋值 $v_{z_0}(f)$ 重新叙述这些定义:

$$v_{z_0}(f) = \inf\{n \in \mathbf{Z}, a_n \neq 0\} \in \mathbf{Z} \cup \{\pm\infty\}.$$

于是有

- $v_{z_0}(f) = -\infty \Leftrightarrow f$ 在 z_0 有一个本性奇点;
- $v_{z_0}(f) > -\infty \Leftrightarrow f$ 在 z_0 为亚纯的;
- $v_{z_0}(f) = -k,\ k \in \mathbf{N} - \{0\} \Leftrightarrow f$ 在 z_0 有一个 k 阶极点;
- $v_{z_0}(f) \geqslant 0 \Leftrightarrow f$ 在 z_0 为全纯的;
- $v_{z_0}(f) = 0 \Leftrightarrow f$ 在 z_0 为全纯的并在 z_0 不为 0;
- $v_{z_0}(f) = k, k \in \mathbf{N} \Leftrightarrow f$ 在 z_0 有一个 k 阶零点;
- $v_{z_0}(f) = +\infty \Leftrightarrow f$ 在 Ω 的包含 z_0 的连通分支上为零.

在上面的这些等价关系中唯一不是那些定义的重述的是最后那一个, 它是孤立零点定理 (定理 V.3.3) 的重述.

如果 Ω 是 $\mathbf{C}$ 的一个开集, 称 $f : \Omega \to \mathbf{C}$ 在 Ω 上为亚纯的是说 f 在 Ω 的每一点都为亚纯的.

对于某一些应用, 显式地计算出 f 在 z_0 的留数是重要的. 以下的习题提供了一些计算方案[10].

习题 VI.3.5. — 设 Ω 是 $\mathbf{C}$ 的一个开集, 且 $z_0 \in \Omega$.

(i) 如果 f 在 z_0 全纯, 则 $\mathrm{Res}(f, z_0) = 0$.

(ii) 如果 $f = \frac{g}{h}$, 其中 g 和 h 在 Ω 上全纯, 如果 $g(z_0) \neq 0$ 而 h 在 z_0 具单零点, 则 $\mathrm{Res}(f, z_0) = \frac{g(z_0)}{h'(z_0)}$.

(iii) 如果 f 在 z_0 有一个单极点, 且 g 在 z_0 全纯, 则 $\mathrm{Res}(fg, z_0) = g(z_0)\mathrm{Res}(f, z_0)$.

(iv) 如果 $k \geqslant 1$, 而 $f = (z - z_0)^{-k} g$, 其中 g 在 Ω 全纯, 则 $\mathrm{Res}(f, z_0) = \frac{g^{(k-1)}(z_0)}{(k-1)!}$.

[392] (v) 如果 f 在 Ω 亚纯, 则 $\frac{f'}{f}$ 在 Ω 也亚纯, 具有单极点且在 f 的极点和零点处, 并对任意的 $z_0 \in \Omega$ 有

$$\mathrm{Res}\left(\frac{f'}{f}, z_0\right) = v_{z_0}(f).$$

习题 VI.3.6. — 设 $\lambda \in \mathbf{R}_+^*$. 计算 $\mathrm{Res}(\frac{1}{z^2+\lambda^2} e^{1/z}, 0)$.

习题 VI.3.7. — 证明: f 在 Ω 上亚纯当且仅当对 Ω 上每一个点 z_0 有一个开邻域[11] U, 其中 g, h 在 U 上全纯.

习题 VI.3.8. — 设 $f : \Omega \to \mathbf{C}$ 亚纯.

---

[10] 如果 f 有一个本性奇点, 一般则不可能找到留数的一个 "有限" 表达式, 其理由之一是有一些积分不能用于留数方法 (参看 4 小节的习题)

[11] 可以证明可将 f 写成 $f = \frac{g}{h}$, 其中 g 和 h 在整个 Ω 上全纯, 但对于任意的开集 Ω 而言, 这远非显然.

(i) 证明 f 的极点为孤立的 (即, 如果 a 是一个极点, 则存在 $r>0$ 使得 a 在邻域 $D(a,r^-)$ 中为 f 的单极点).

(ii) 证明 f 在 $D(x_0,r)\subset\Omega$ 中只有有限个极点.

习题 VI.3.9. — (i) 证明一个在无限远有界的亚纯函数 (即, 存在 M 和 R 使得当 $|z|\geqslant R$ 时有 $|f(z)|\leqslant M$) 是一个有理分式. (先证明 f 只有有限个极点.)

(ii) 证明在无限远处趋向无穷大的一个亚纯函数是一个有理分式.

习题 VI.3.10. — 设 $(x_n)_{n\in\mathbf{N}}$ 是 $\mathbf{C}^*$ 中趋向无穷的序列, 而 $(k_n)_{n\in\mathbf{N}}$ 是 $\mathbf{N}$ 中的一个序列.

(i) 证明存在 $a_n\in\mathbf{N}$ 使得当 $|z|<\frac{|x_n|}{2}$ 时有

$$\left|\left(\left(1-\frac{z}{x_n}\right)e^{\frac{z}{x_n}+\frac{z^2}{2x_n^2}+\cdots+\frac{z^{a_n}}{a_nx_n^{a_n}}}\right)^{k_n}-1\right|\leqslant 2^{-n}.$$

(ii) 在 $\mathbf{C}$ 上构造一个全纯函数使它的零点为 x_n 而阶数为 k_n.

(iii) 证明 $\mathbf{C}$ 上的所有亚纯函数都是 $\mathbf{C}$ 上的两个全纯函数的商.

(iv) 修改上述方法, 证明在 $D(0,1^-)$ 上的亚纯函数是 $D(0,1^-)$ 上的两个全纯函数的商.

习题 VI.3.11. — 设 $R>0$ 而 f 在 $D(z_0,R^-)-\{z_0\}$ 上全纯. 证明

(i) f 在 z_0 全纯当且仅当 f 对任意的 $r\in]0,R[$ 在 $D(z_0,r)-\{z_0\}$ 中有界 (可以关注一下 $\int_{C(z_0,r)}(z-z_0)^{-n-1}f(z)dz$).

(ii) f 在 z_0 为亚纯的但非全纯的当且仅当在 $z\to z_0$ 时有 $|f(z)|\to+\infty$.

(iii) f 在 z_0 是本性奇异的当且仅当对任意的 $r\in]0,R[$ 有 $D(z_0,r^-)-\{z_0\}$ 在 f 下的像稠密[12] 于 $\mathbf{C}$.

习题 VI.3.12. — (i) 设 $f:\mathbf{C}\to\mathbf{C}$ 全纯. 利用前面的习题证明, 如果 f 不是多项式, 则 $f(\mathbf{C}-D(0,n))$ 是 $\mathbf{C}$ 的一个稠开集, 其中 $n\in\mathbf{N}$ 任意. 由此推出 f 不是一个单射.

(ii) 证明, 如果 $f:\mathbf{C}\to\mathbf{C}$ 为全纯的双射, 则存在 $a\in\mathbf{C}^*, b\in\mathbf{C}$ 使得对任意的 $z\in\mathbf{C}$ 有 $f(z)=az+b$.

3. 留数公式 [393]

定理 VI.3.13. — 设 Ω 是 $\mathbf{C}$ 的一个开集, F 是 Ω 的有限个点的集合, 而 f 在 $\Omega-F$ 中全纯, 并设 γ 是 Ω 中的一条在 Ω 中收缩的闭道且不与 F 相交, 于是

$$\int_\gamma f(z)dz=2i\pi\sum_{a\in F}I(\gamma,a)\mathrm{Res}(f,a).$$

[12]"皮卡大定理" 断言, $D(z_0,r^-)-\{z_0\}$ 在 f 下的像最多除去一个点外包含了 $\mathbf{C}$. (例子 $e^{1/z}$ 表明这个定理达到最佳). 此定理的证明需要用到有点超出本书的复杂技术.

证明 如果 $a \in F$ 及 $r_a > 0$ 使得 $D(a, r_a^-)$ 包含在 Ω 中而不包含 F 中其他的点, 于是存在一个 $\mathbf{C}$ 中的序列 $(c_{a,n})_{n\in\mathbf{Z}}$ 使得当 $z \in D(a, r_a^-)$ 中时有 $f(z) = \sum_{n\in\mathbf{Z}} c_{a,n}(z-a)^n$. 又, 级数 $\sum_{n\leqslant -2} c_{a,n}(z-a)^n$ 定义了 $\mathbf{C} - \{a\}$ 上的一个全纯函数 g_a, 而 g_a 在 $\mathbf{C} - \{a\}$ 上有原函数 $G_a(z) = \sum_{n\leqslant -2} c_{a,n}\frac{(z-a)^{n+1}}{n+1}$. 于是令 $h = f - \sum_{a\in F}(g_1 + \frac{C_{a,-1}}{z-a})$. 由构造, h 在 $\Omega - F$ 上全纯, 并在 F 中的每点上具有可去奇点; 因此可连续地延拓到整个 Ω 上. 于是有

- $\int_\gamma f(z)dz = \int_\gamma h(z)dz + \sum_{a\in F}\int_\gamma g_a(z)dz + \sum_{a\in F} c_{a,-1}\int_\gamma \frac{dz}{z-a}$;
- $\int_\gamma h(z)dz = 0$: 因为 h 在 Ω 上全纯且 γ 在 Ω 上可缩;
- 如果 $a \in F$, 则 $\int_\gamma g_a(z)dz = 0$: 因为 g_a 在包含了 γ 的 $\Omega - \{a\}$ 上具有一个原函数;
- 由定义, $c_{a,-1} = \mathrm{Res}(f, a)$ 和 $\int_\gamma \frac{dz}{z-a} = 2i\pi I(\gamma, a)$.

定理得证. □

留数公式可定位一个全纯函数的零点.

推论 VI.3.14. — 设 $\Omega \subset \mathbf{C}$ 为开集, 且 $z_0 \in \Omega$ 及 $r > 0$ 使得 $D(z_0, r) \subset \Omega$. 又设 f 在 Ω 上全纯. 如果 $C(z_0, r)$ 不包含 f 的零点, 则 f 在 $D(z_0, r)$ 中的带重数的零点数等于 $\frac{1}{2i\pi}\int_{C(z_0,r)}\frac{f'(z)}{f(z)}dz$.

证明 我们已知 (参看习题 VI.3.5 的 (v)), $\frac{f'(z)}{f(z)}$ 在 Ω 上为亚纯的, 其在 f 的零点上有单极点, 并且在这些极点上的留数是 f 的零点的阶. 于是留数公式给出了结果 □

4. 习题

习题 VI.3.15. — 设 f 在 $\mathbf{R}$ 上由 $f(t) = e^{-\pi t^2}$ 定义. 回想, 已知 $\int_{\mathbf{R}} e^{-\pi t^2}dt = 1$.

(i) 证明 f 可解析延拓为 $\mathbf{C}$ 上的一个全纯函数 (仍记为 f).

(ii) 如果 $a \in \mathbf{R}$ 和 $R \in \mathbf{R}_+$, 设 $\gamma_{a,R}$ 为由线段 $[-R, R], [R, R+ai], [R+ai, -R+ai]$ 和 $[-R+ai, -R]$ 连接成的闭道. $\int_{\gamma_{a,R}} f(z)dz$ 的值是什么?

(iii) 令 R 趋向 $+\infty$, 并由此推出 $\hat{f}(a) = e^{-\pi a^2}$.

习题 VI.3.16. — 用留数方法计算以下积分:

(a) $\int_{\mathbf{R}}\frac{dx}{(x^2+1)(x^2+4)(x^2+9)}$ 和 $\int_{\mathbf{R}}\frac{dx}{(x+i)(x-i)(x-2i)\cdots(x-ni)}$. (取由线段 $[-R, R]$ 和一个适当的半圆组成的闭道 γ.)

(b) $\lim_{R\to+\infty}\int_{-R}^{R}\frac{x^3}{(x^2+1)(x^2+x+1)}dx$.

[394] (c) $\int_0^{+\infty}\frac{x^a}{x^b+1}dx$, 其中 $a, b \in \mathbf{N}$ 且 $b \geqslant a+2$. (取由线段 $[0, R]$, 一段适当的圆弧, 以及线段 $[Re^{i\alpha}, 0]$ (其中 α 需恰当选取) 组成的闭道.)

习题 VI.3.17. — (有理函数的傅里叶变换)

(i) 用留数方法计算 $\int_{\mathbf{R}}\frac{e^{-2i\pi t\xi}}{t^2+1}dt$ 和 $\int_{\mathbf{R}}\frac{e^{-2i\pi t\xi}}{(t+i)^2}dt$. (取由线段 $[-R, R]$ 和一个适当

的半圆[13] 组成的闭道 γ.)

(ii) 同样计算 $\lim_{R\to+\infty}\int_{-R}^{R}\frac{te^{-2i\pi t\xi}}{t^2+t+1}dt$.

习题 VI.3.18. — 设 $\gamma_{\varepsilon,R}$ 是由线段 $[\varepsilon,R]$, 半圆 $C^+(0,G):[0,\pi]\to\mathbf{C}$, 它由 $t\mapsto Re^{it}$ 给出, 线段 $[-R,-\varepsilon]$, 以及由 $t\mapsto\varepsilon e^{i(\pi-t)}$ 给出的半圆 $C^+(0,\varepsilon)^{\mathrm{opp}}$ 连接成的闭道.(请作图.)

(i) 用留数公式计算 $\int_{\gamma_{\varepsilon,R}}\frac{e^{iz}}{z}dz$.

(ii) 证明当 $R\to+\infty$ 时有 $\int_{C^+(0,R)}\frac{e^{iz}}{z}dz\to 0$.

(iii) 计算当 $\varepsilon\to 0$ 时 $\int_{C^+(0,\varepsilon)^{\mathrm{opp}}}\frac{e^{iz}}{z}dz$ 的极限.

(iv) 由此得到 $\int_0^{+\infty}\frac{\sin x}{x}dx=\frac{\pi}{2}$.

习题 VI.3.19. — 我们要证明 $\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin\pi s}, s\neq\mathbf{Z}$ (余元公式[14]), 其中的 Γ 是在习题 V.5.9 中定义的 $\mathbf{C}-\mathbf{N}$ 上的全纯函数.

(i) 设 s 在带状区域 $-1<\mathrm{Re}(s)<0$ 中.(可以在后面修改它以便计算 $\int_0^{+\infty}f(t)t^s dt$, 其中 f 是一个有理分式). 如果 $r>0$, 以 $C^+(0,r)$ 记圆 $\theta\mapsto re^{i\theta}$ 的四分之一的部分, $\theta\in[0,\frac{\pi}{2}]$, 以 $C^-(0,r)$ 记圆 $\theta\mapsto re^{i\theta}$ 的四分之三的部分, $\theta\in[\frac{\pi}{2},2\pi]$. 如果 $0<\varepsilon<R$, 令 $\gamma^+_{\varepsilon,R}$ 为由 $C^+(0,R),[iR,i\varepsilon],C^+(0,\varepsilon)^{\mathrm{opp}}$ 和 $[\varepsilon,R]$ 连接成的闭道 (请作图!), 并令 $\gamma^-_{\varepsilon,R}$ 为由 $[i\varepsilon,iR],C^-(0,R),[R,\varepsilon]$ 和 $C^-(0,\varepsilon)^{\mathrm{opp}}$ 连接成的闭道.

(a) 利用留数公式计算 $\int_{\gamma^+_{\varepsilon,R}}\frac{(-z)^s}{z+1}dz$ 和 $\int_{\gamma^-_{\varepsilon,R}}\frac{(-z)^s}{z+1}dz$, 其中当 $z\in\mathbf{R}^*_-$ 时 $\log(-z)\in\mathbf{R}$. (注意对数主分支!)

(b) 证明当 $\varepsilon\to 0$ 和 $R\to+\infty$ 时这些积分在圆的这些部分上的积分趋向 0.

(c) 由此得到当 $-1<\mathrm{Re}(s)<0$ 时, $\int_0^{+\infty}\frac{y^s}{y+1}dy$ 的值.

(ii) 设 $B(s,t)=\int_0^1 x^{s-1}(1-x)^{t-1}dx$. 证明当 $\mathrm{Re}(s)>0$ 且 $\mathrm{Re}(t)>0$ 时有 $B(s,t)=\frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}$. (将 $\Gamma(s+t)B(s+t)$ 表示为一个二重积分.)

(iii) 证明余元公式 (利用经变量变换 $y=\frac{x}{x-1}$ 得到的公式 $B(s,t)=\int_0^{+\infty}\frac{y^{s-1}}{(1+y)^{s+t}}dy$.)

习题 VI.3.20. — 用留数公式计算 $\int_0^{+\infty}\frac{\log t}{(t+1)(t+2)}dt$. (计算 $\frac{(\log z)^2}{(z+1)(z+2)}dz$ 在习题 VI. 3.19 的那些闭道上的积分.)

习题 VI.3.21. — 设 $P\in\mathbf{C}[X]$ 为 n 次首 1 多项式. 计算

$$\lim_{R\to+\infty}\frac{1}{2i\pi}\int_{C(0,R)}\frac{P'(z)}{P(z)}dz.$$

由此推得 $\mathbf{C}$ 为代数闭域.

习题 VI.3.22. — 设 Ω 是 $\mathbf{C}$ 的一个连通开集. 又设 f 是在 Ω 上不恒为 0 的一个全纯函数, 而 f_n 是在 Ω 的每个紧集上一致趋向 f 的全纯函数的序列.

[13]取一个适当的半圆的方式是要使当 $|\xi|\to+\infty$ 时所得到的在半圆上的积分趋向 0; 还应该关注闭道对于这些极点的指标 ……

[14]它的另外的证明可在习题 VII.2.2 和 H.1.11 中找到.

[395] (i) 设 $z_0 \in \Omega$, $r > 0$ 使得 $D(z_0, r) \subset \Omega$. 假设 $C(z_0, r)$ 不包含 f 的任一个零点. 证明存在 $N(z_0, r)$ 使得当 $n \geqslant N(z_0, r)$ 时有 f 和 f_n 在 $D(z_0, r^-)$ 中具有计入了重数的相同的零点数.

(ii) 证明, 如果 f_n 对所有充分大的 n 在 Ω 上为单值的, 则 f 也如此.

习题 VI.3.23. — (鲁歇 (Rouché) 定理及其应用)

设 $R > 0, D = D(0, R)$ 以及 $C = \partial D = C(0, R)$. 又设 Ω 是一个包含 D 的开集, f 在 Ω 上全纯, 并在 C 上不取零, 而 g 在 Ω 上全纯, 使得当 $z \in C$ 时, $|f(z) - g(z)| < |f(z)|$.

(i) 证明存在包含 C 的开集基 $\Omega' \subset \Omega$ 和在 Ω' 上的全纯函数 h 使得在 Ω' 上有 $\frac{g}{f} = e^h$. h' 的值是什么?

(ii) 证明 f 和 g 在 D 中具有相同的零点数 (计入重数) (鲁歇定理). 这个结果只对圆盘成立吗?

(iii) 设 G 在 Ω 上全纯使得当 $z \in C$ 时 $|G(z)| < R$. 证明 $G(D) \subset D$ 且 G 在 D 中有唯一的不动点.

(iv) 证明 $z \sin z = 1$ 的解是实数.

习题 VI.3.24. — 设 Γ 是 $\mathbf{C}$ 上的亚纯函数, 除在负整数上的单极点外为全纯的, 它在 $\mathrm{Re}(z) > 0$ 上的定义是 $\Gamma(z) = \int_0^{+\infty} e^{-t} t^z \frac{dt}{t}$. 记得 (参看习题 V.5.9) 有 $\Gamma(z) = \frac{\Gamma(z+n+1)}{z(z+1)\ldots(z+n)}$, 其中 $n \in \mathbf{N}$ 任意.

(i) 证明 $\lim_{z \to -n} (z+n)\Gamma(z) = \frac{(-1)^n}{n!}$.

(ii) 证明, 如果 $x > 0$ 而 $c \notin -\mathbf{N}$, 则 $I_c(x) = \int_{c-i\infty}^{c+i\infty} x^{-z}\Gamma(z) dz$ 收敛.

(iii) 如果 $n \in \mathbf{N}$, 用留数方法计算 $I_1(x) - I_{\frac{1}{2}-n}(x)$.

(iv) 证明 $I_{\frac{1}{2}-n} \to 0$. 由此推出 $\frac{1}{2i\pi} \int_{1-i\infty}^{1+i\infty} x^{-z}\Gamma(z) dz = e^{-x}$.

(v) 利用傅里叶变换重新证明这个结果.

习题 VI.3.25. — 如果 $N \in \mathbf{N}$, 设 C_N 为顶点 $(2N+1)\pi(\pm 1 \pm i)$ 的正方形的沿正方向的边界, 并令 $I_N = \int_{C_N} \frac{dz}{z^2(e^z - 1)}$.

(i) 利用留数公式计算 I_N.

(ii) 证明当 $N \to +\infty$ 时有 $I_N \to 0$.

(iii) 由此得到公式 $\zeta(2) = \frac{\pi^2}{6}$.

(iv) 设对于 $n \in \mathbf{N}$, B_n 由 $\frac{z}{e^z - 1} = \sum_{n=0}^{+\infty} B_n \frac{z^n}{n!}$ 定义. 修改前面的证明, 计算用函数 B_n 表达的 $\zeta(2k)$, $k \in \mathbf{N} - \{0\}$. 由此得到 $\pi^{-2k}\zeta(2k) \in \mathbf{Q}$.

习题 VI.3.26. — 计算沿顶点为 $(N + \frac{1}{2})(\pm 1 \pm i)$ 的正方形 (边) 上函数 $\frac{\pi \cot \pi z}{(z^2+1)^2}$ 的积分. 由此算出 $\sum_{n \in \mathbf{Z}} \frac{1}{(n^2+1)^2}$ 的值.

习题 VI.3.27. — ($\frac{1}{\cosh \pi t}$ 的傅里叶变换)

以两种方法计算 $\int_{\mathbf{R}} e^{2i\pi t\xi}\frac{e^{\pi t}}{e^{2\pi t}+1}dt$: 一方面在适当的矩形上对 $e^{2i\pi z\xi}\frac{e^{\pi z}}{e^{2\pi z}+1}dz$ 积分, 然后让顶点趋向无限, 另一方面, 将 $\frac{e^{\pi t}}{e^{2\pi t}+1}$ 按 t 为负或正写成 $e^{\pi t}$ 或 $e^{-\pi t}$ 的级数. 与习题 V.5.3 比较.

习题 VI.3.28. — (高斯积分和二次互反律)

这个习题应用留数方法给出了公式 $\int_{\mathbf{R}} e^{-\pi t^2}dt = 1$ 的证明和二次互反律的一个证明.

(i) 以 I 记积分 $\int_{\mathbf{R}} e^{-\pi t^2}dt$, 且若 $a \in \mathbf{N} - \{0\}$, 令 $G(a) = \sum_{k\in\mathbf{Z}/a\mathbf{Z}} e^{2i\pi\frac{k^2}{a}}$.

(a) 证明 $z \mapsto F(z) = \int_{\mathbf{R}} e^{-\pi t^2}e^{-2i\pi tz}dt$ 在 $\mathbf{C}$ 上全纯.

(b) 如果 $y \in \mathbf{R}$, 计算 $F(iy)$; 由此得到, 对所有的 $z \in \mathbf{C}$ 有 $F(z) = Ie^{-\pi z^2}$.

(c) 设 $\Phi_a(z) = \sum_{k=0}^{2a-1} e^{-2\pi az^2}e^{2\pi k\omega z}$, 其中 $\omega = \frac{1+i}{\sqrt{2}}$. 证明 $\int_{\mathbf{R}} \Phi_a(t)dt = \frac{1}{\sqrt{8a}}G(4a)$. [396] (先证明 $\int_{\mathbf{R}} e^{-2\pi at^2}e^{2\pi k\omega t}dt = \frac{1}{\sqrt{2a}}e^{2i\pi\frac{k^2}{4a}}$.)

(ii) 如果 $a \in \mathbf{N} - \{0\}$, 令 $\Psi_a(z) = \frac{e^{-2\pi az^2}}{e^{2i\pi\frac{z}{\omega}}-1}$.

(a) 证明 $\Psi_a(z-\omega) - \Psi_a(z) = \Phi_a(z)$.

(b) 用留数方法计算 $\int_{\mathbf{R}} \Psi_a(t-\frac{\omega}{2})dt - \int_{\mathbf{R}} \Psi_a(t+\frac{\omega}{2})dt$.

(c) 由此得到 $\frac{1}{\sqrt{8a}}G(4a) = \omega$, 而后有 $I = 1$.

(iii) 如果 p 是素数且 $(n,p) = 1$, 则按照 n 是否是 $\mathbf{F}_p$ 中的平方数定义勒让德符号 $(\frac{n}{p}) = 1$ 或 -1. 又令 $G_n(p) = \sum_{k\in\mathbf{F}_p} e^{2i\pi\frac{nk^2}{p}}$. 回想: 我们已知, 如果 a, b 互素, 则 $(x,y) \mapsto bx+ay$ 诱导了一个双射 $(\mathbf{Z}/a\mathbf{Z}) \times (\mathbf{Z}/b\mathbf{Z}) \cong \mathbf{Z}/ab\mathbf{Z}$.

(a) 当 a 为奇数时, 建立联系 $G(4a)$ 和 $G(a)$ 的关系; 由此得到, 当 $a \equiv 1 \mod 4$ 时, $G(a) = \sqrt{a}$; 而当 $a \equiv 3 \mod 4$ 时, $G(a) = i\sqrt{a}$ (高斯的公式).

(b) 证明 $\sum_{m\in\mathbf{F}_p} e^{2i\pi\frac{m}{p}} = 0$; 由此得到, 当 $(n.p) = 1$ 时有 $G_n(p) = (\frac{n}{p})G(p)$.

(c) 设 $p \neq q$ 是两个奇素数. 证明 $G(pq) = (\frac{q}{p})(\frac{p}{q})G(p)G(q)$; 由此得到二次互反律 $(\frac{q}{p})(\frac{p}{q}) = (-1)^{(p-1)(q-1)/4}$.

VII. 狄利克雷级数

一个广义的狄利克雷 (Dirichlet) 级数是一个形如 $\sum_{n=1}^{+\infty} a_n e^{-\lambda_n s}$ 的级数, 其中 a_n 是复数, 而 λ_n 是其实部趋向 $+\infty$ 的复数. (如果对所有的 n 有 $\lambda_n = n-1$, 则当 mod 变量变换 $e^{-s} = z$ 时, 我们便重新回到了整级数的情形 (其中的指标有些不自然), 这让我们可将广义的狄利克雷级数看为整级数的推广.) 在本章中, 我们只对所有的 n 有 $\lambda_n = \log n$ 的情形感兴趣, 而这正是狄利克雷原来考虑的情形, 但, 譬如当试图定义一个无穷维算子的行列式时就会自然地涉及广义的狄利克雷级数, 这在数学和物理学中有许多的应用[1]. 作为这个 "ζ 正则化 (zeta-regulation)" 方法的一个例证, 我们提出的是, 公式

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots = \sqrt{2\pi}$$

等价于 $-\sum_{n=1}^{+\infty} \log n = -\frac{1}{2}\log 2\pi$, 而其中的左端被解释为函数 ζ 在 0 的导数, 而这个 ζ 是已被解析延拓到了 $\mathbf{C} - \{1\}$ 上的函数[2] $\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}, \mathrm{Re}(s) > 1$.

VII.1. 狄利克雷级数

1. 绝对收敛的横坐标

我们称形如 $L(\boldsymbol{a}, s) = \sum_{n=1}^{+\infty} a_n n^{-s}$ 的级数为狄利克雷级数, 其中 $s \in \mathbf{C}$, $\boldsymbol{a} = (a_n)_{n \geqslant 1}$ 是一个复数序列 (且 $n^{-s} = \exp(-s\log n)$, 而 $\log n \in \mathbf{R}_+$). 一个狄利克雷级数可以对任何 s 值不收敛, 但如果对 s_0 收敛, 则特别有 $a_n n^{-s_0} \to 0$, 因此

---

[1] 一个振动的膜的频率是在代表此膜的 $\mathbf{C}$ 中开集上的拉普拉斯算子的特征值. 拉普拉斯算子的 ζ 函数 $\zeta_\Delta(s) = \sum \lambda^{-s}$, 其中的和号取在非零特征值上, 这个函数解开了频率与曲面几何间的关系. 拉普拉斯的行列式为 $\exp(-\zeta'_\Delta(0))$; 它涉及, 例如, 重正规化 (renormalisation) 问题.

[2] 这个解析延拓的存在性是定理 VII.3.4 的课题, 而公式 $\zeta'(0) = -\frac{1}{2}\log 2\pi$ 的证明则在习题 VII.3.9 中提及.

[398] $|a_n| = o(n^{\mathrm{Re}(s_0)})$. 反之, 如果对某个 $\alpha \in \mathbf{R}$ 有 $|a_n| = O(n^\alpha)$, 则 $\sum_{n=1}^{+\infty} a_n n^{-s}$ 在形如 $\mathrm{Re}(s) > \alpha + 1 + \delta, \delta > 0$ 的整个半平面上按范数收敛, 因此它在半平面 $\mathrm{Re}(s) > \alpha + 1$ 上定义了一个全纯函数. 同样, 如果 $\sum_{n=1}^{+\infty} a_n n^{-s}$ 对于 $s = s_0$ 绝对收敛, 则它在半平面 $\mathrm{Re}(s - s_0) \geqslant 0$ 上按范数收敛: 因为在此半平面上 $|a_n n^{-s}| \leqslant |a_n n^{-s_0}|$; 因此它在开的半平面 $\mathrm{Re}(s - s_0) > 0$ 上定义了一个全纯函数, 并连续地延拓到了闭的半平面 $\mathrm{Re}(s - s_0) \geqslant 0$ 上.

上面的讨论自然地引出了 $\overline{\mathbf{R}}$ 中的如下一些元的定义:

- 收敛横坐标: $\sigma_{\mathrm{conv}} = \inf\{\mathrm{Re}(s), L(\boldsymbol{a}, s)$ 收敛$\}$;
- 绝对收敛横坐标: $\sigma_{\mathrm{abs}} \inf\{\mathrm{Re}(s), L(\boldsymbol{a}, s)$ 绝对收敛$\}$;
- $\sigma_{\mathrm{hol}} = \inf\{\sigma \in \mathbf{R}, L(\boldsymbol{a}, s)$ 在 $\mathrm{Re}(s) > \sigma$ 上有一个解析延拓$\}$;
- $\tau = \inf\{\alpha \in \mathbf{R}, a_n = O(n^\alpha)\}$.

数 τ 没有什么特别的意义, 只不过在前面这些量中它是最容易算出的; 另外, 上面的讨论给出了一个上下的界限:

$$\tau \leqslant \sigma_{\mathrm{conv}} \leqslant \sigma_{\mathrm{abs}} \leqslant \tau + 1.$$

又, 与整级数情形相反 (参看注记 V.4.9 的 (i)), 就像狄利克雷 L 函数 (定理 VII. 4.4) 表明的那样, 我们不必有 $\sigma_{\mathrm{hol}} = \sigma_{\mathrm{abs}}$. 对于许多从数论或理论物理来的狄利克雷级数, 人们猜想 $\sigma_{\mathrm{hol}} = -\infty$ (即存在在整个复平面上的解析延拓), 这有点出人意料, 它显示了隐藏在背后的对称性, 而这个对称性仍然十分神秘.

在整个后文中我们假定所考虑的狄利克雷级数均在某处收敛 (即 $\sigma_{\mathrm{abs}} \neq +\infty$), 而在相反的情形没有多少意思 …… 因此这时我们可以从函数 $L(\boldsymbol{a}, s)$ 重新找出 a_n (事实上, $a_1 = \lim_{s\to+\infty} L(\boldsymbol{a}, s)$, $a_2 = \lim_{s\to+\infty} 2^s(L(\boldsymbol{a}, s) - a_1)$, 等等).

我们还注意到, 两个狄利克雷级数的乘积 $L(\boldsymbol{a}, s)L(\boldsymbol{b}, s)$ 仍然是一个狄利克雷级数 $L(\boldsymbol{c}, s) = \sum_{n\geqslant 1} \frac{c_n}{n^s}$, 其中 $c_n = \sum_{d|n} a_d b_{n/d}$. 这个涉及整数分解的公式应归功于算术问题对于狄利克雷级数的兴趣.

定理 VII.1.1. — (兰道 (Landau)) 设 $L(\boldsymbol{a}, s) = \sum_{n\geqslant 1} \frac{a_n}{n^s}$ 是一个正系数 (即对所有的 $n \geqslant 1$ 有 $a_n \in \mathbf{R}_+$) 的狄利克雷级数. 于是 $L(\boldsymbol{a}, s)$ 不可能解析延拓到 σ_{abs} 的任何一个邻域上[3].

推论 VII.1.2. — 如果 $L(\boldsymbol{a}, s) = \sum_{n\geqslant 1} \frac{a_n}{n^s}$ 是一个正系数的狄利克雷级数, 则 $\sigma_{\mathrm{hol}} = \sigma_{\mathrm{abs}}$.

[399] 证明 推论是直接的, 故而转向定理的证明. 令 $\sigma = \sigma_{\mathrm{abs}}$, 并按归谬法假定存在 $\varepsilon > 0$ 使得 $L(\boldsymbol{a}, s)$ 具有一个到圆盘 $D(\sigma, (3\varepsilon)^-)$ 的解析延拓. 于是 $L(\boldsymbol{a}, s)$ 在 $D(\sigma, (3\varepsilon)^-)$ 和上半平面 $\mathrm{Re}(s) > \sigma$ 的并的开集 Ω 上全纯. 由于 Ω 包含了 $D(\sigma + \varepsilon, (3\varepsilon)^-)$,

[3] 可以出现 $L(\boldsymbol{a}, s)$ 具有一个亚纯延拓, 这就像黎曼 ζ 函数的情形的证明那样 (参看定理 VII.3.4), 这时 σ_{abs} 是这个延拓的极点.

于是 $L(\boldsymbol{a},s)$ 是在这个圆盘上在 $\sigma+\varepsilon$ 的泰勒展开式的和, 故有 $L(\boldsymbol{a},\sigma-\varepsilon)=\sum_{k=0}^{+\infty}\frac{L^{(k)}(\boldsymbol{a},\sigma+\varepsilon)}{k!}(-2\varepsilon)^k$. 另外, 因为 $\sigma+\varepsilon$ 是在 $L(\boldsymbol{a},s)$ 的收敛半平面中, 故根据定理 V.5.1, 用对这个狄利克雷级数逐项取导数的方法来计算 $L^{(k)}(\boldsymbol{a},\sigma_\varepsilon)$. 因此得到

$$L(\boldsymbol{a},\sigma-\varepsilon)=\sum_{k=0}^{+\infty}L^{(k)}(\boldsymbol{a},\sigma+\varepsilon)\frac{(-2\varepsilon)^k}{k!}=\sum_{k=0}^{+\infty}\left(\sum_{n=1}^{+\infty}\frac{a_n(-\log n)^k}{n^{\sigma+\varepsilon}}\right)\frac{(-2\varepsilon)^k}{k!}.$$

将 $(\frac{-2\varepsilon)^k}{k!}$ 放回括号里面, 便得到一个具正项的二重级数, 这时便可交换取和的次序得到

$$L(\boldsymbol{a},\sigma-\varepsilon)=\sum_{n=1}^{+\infty}\frac{a_n}{n^{\sigma+\varepsilon}}\left(\sum_{k=0}^{+\infty}\frac{(2\varepsilon\log n)^k}{k!}\right)=\sum_{n=1}^{+\infty}\frac{a_n}{n^{\sigma+\varepsilon}}n^{2\varepsilon}=\sum_{n=1}^{+\infty}\frac{a_n}{n^{\sigma-\varepsilon}}.$$

由此得到 $L(\boldsymbol{a},s)$ 在 $\sigma-\varepsilon$ 收敛, 这与 σ 的定义矛盾. 定理得证. □

2. 狄利克雷级数的收敛半平面

与整级数相反, 一般地有[4] $\sigma_{\text{conv}}\neq\sigma_{\text{abs}}$, 而确定 σ_{conv} 可能隐藏有巨大的困难…… 另一方面, 根据后面的推论 VII.1.6, 我们有 $\sigma_{\text{hol}}\leqslant\sigma_{\text{conv}}$, 但对于狄利克雷的 L 函数的情形 (定理 VII.4.4) 可以证明这个等号总不成立. 这与整级数情形相反. 数 σ_{hol} 常常是极其难于计算的. 朗兰兹 (Langlands) 纲领 (参看附录 G) 的一大部分是想要证明, 对于来自数论的许多狄利克雷级数有 $\sigma_{\text{hol}}=-\infty$.

狄利克雷级数收敛性的研究基于下面的引理.

引理 VII.1.3. — 设 $\alpha,\beta\in\mathbf{R}$, 满足 $0<\alpha<\beta$. 设 $z=x+iy$, $x,y\in\mathbf{R}$, 且 $x>0$. [400] 于是

$$|e^{-\alpha z}-e^{-\beta z}|\leqslant|\frac{z}{x}|(e^{-\alpha x}-e^{-\beta x}).$$

证明 我们有 $e^{-\alpha z}-e^{-\beta z}=z\int_\alpha^\beta e^{-tz}dt$, 因此

$$|e^{-\alpha z}-e^{-\beta z}|\leqslant|z|\int_\alpha^\beta e^{-tx}dt=|\frac{z}{x}|(e^{-\alpha x}-e^{-\beta x}).$$

□

将此引理用于 $\alpha=\log n$, $\beta=\log(n+1)$, 而 $z=s-s_0$ 便得到下面的推论.

[4] 例如, 假设 $a_n\in\{\pm\}$, $n\geqslant1$. 于是有 $\sigma_{\text{abs}}=1$. 为了研究 σ_{conv}, 可以利用阿贝尔求和公式: 令 $A_n=\sum_{k=1}^n a_k$ 使得

$$\sum_{n=1}^N\frac{a_n}{n^s}=\frac{A_N}{(N+1)^s}+\sum_{n-1}^N A_n(n^{-s}-(n+1)^{-s})=\frac{A_N}{n^{s+1}}+\sum_{n=1}^N\frac{A_n}{n^{s+1}}(n(1-(1+\frac{1}{n})^{-s})).$$

由此得到, 如果 $A_n=O(n^\alpha),\alpha<1$, 则 $\sigma_{\text{conv}}\leqslant\alpha$, 然而豪斯多夫 (1913) 证明, 几乎肯定 (将这些 a_n 考虑为取值在 $\{\pm\}$ 中的具有相等概率的独立的随机变量), 对于任意的 $\varepsilon>0$ 有 $A_n=O(n^{\frac{1}{2}+\varepsilon})$, 从而几乎肯定有 $\sigma_{\text{conv}}\leqslant1/2$ (而 $1/2$ 当然不同于 1).

推论 VII.1.4. — 如果 $n \geqslant 1$, 且若 $\mathrm{Re}(s-s_0)>0$, 则

$$|n^{-(s-s_0)}-(n+1)^{-(s-s_0)}| \leqslant \frac{|s-s_0|}{\mathrm{Re}(s-s_0)}\left(n^{-\mathrm{Re}(s-s_0)}-(n+1)^{-\mathrm{Re}(s-s_0)}\right).$$

定理 VII.1.5. — 设 $L(\boldsymbol{a},s)=\sum_{n=1}^{+\infty}a_n n^{-s}$ 为一个狄利克雷级数, 而 $s_0\in\mathbf{C}$.

(i) 如果部分和序列 $A_n(s_0)=\sum_{k=1}^{n}a_k k^{-s_0}$ 有界, 则 $L(\boldsymbol{a},s)$ 在半平面 $\mathrm{Re}(s-s_0)>0$ 的每一个紧集上一致收敛.

(ii) 如果级数 $\sum_{n=1}^{+\infty}a_n n^{-s_0}$ 收敛, 则 $L(\boldsymbol{a},s)$ 在半平面 $\mathrm{Re}(s-s_0)\geqslant 0$ 的所有扇形 $|\arg(s-s_0)|\leqslant\alpha<\frac{\pi}{2}$ 中一致收敛.

证明 在这两种情形下的证明是同样的, 而且此证明主要基于阿贝尔求和公式. 如果 $p,q\in\mathbf{N}$ 且满足 $p\leqslant q$, 则设

$$M_{p,q}=\sup_{p\leqslant n\leqslant q}|B_{n,p}|,\quad 其中\ B_{n,q}=A_n(s_0)-A_{p-1}(s_0)$$

(而因为由约定, 一个空的求和为零, 故 $A_0(s_0)=0$). 我们有

$$\begin{aligned}\sum_{n=p}^{q}a_n n^{-s}&=\sum_{n=p}^{q}(B_{n,p}-B_{n-1,p})n^{-(s-s_0)}\\&=B_{q,p}q^{-(s-s_0)}+\sum_{n=p}^{q-1}B_{n,p}(n^{-(s-s_0)}-(n+1)^{-(s-s_0)}).\end{aligned}$$

如果 $\mathrm{Re}(s-s_0)>0$, 利用推论 VII.1.4 中的控制关系, 不等式 $1\leqslant\frac{|s-s_0|}{\mathrm{Re}(s-s_0)}$ 和 $M_{p,q}$ 的定义, 由此得到控制关系

$$\begin{aligned}|\sum_{n=p}^{q}a_n n^{-s}|&\leqslant M_{p,q}\left(q^{-\mathrm{Re}(s-s_0)}+\frac{|s-s_0|}{\mathrm{Re}(s-s_0)}\sum_{n=p}^{q-1}(n^{-\mathrm{Re}(s-s_0)}-(n+1)^{-\mathrm{Re}(s-s_0)})\right)\\&\leqslant M_{p,q}\frac{|s-s_0|}{\mathrm{Re}(s-s_0)}p^{-\mathrm{Re}(s-s_0)}.\end{aligned}$$

现在, 如果对于任意的 $n\in\mathbf{N}$ 有 $|A_n(s_0)|\leqslant M$, 则对于任意的 $p\leqslant q$ 有 $M_{p,q}\leqslant 2M$. 另外, 如果 K 是半平面 $\mathrm{Re}(s-s_0)>0$ 的一个紧集, 则存在 $a>0$ 和 $b>0$ 使得对于 $s\in K$ 有 $|s-s_0|\leqslant a$ 和 $\mathrm{Re}(s-s_0)\geqslant b$. 因此当 $s\in K$ 时我们有 $|\sum_{n=p}^{q}a_n n^{-s}|\leqslant 2Mab^{-1}p^{-b}$, 这证明了级数 $\sum_{n\geqslant1}a_n n^{-s}$ 满足在 K 上的柯西一致收敛判别准则. 得到了 (i). [401]

为了证明 (ii), 只要注意, 根据柯西判别准则, $\sum_{n\geqslant1}a_n n^{-s_0}$ 收敛的假设等价于当 $p\to+\infty$ 时 $M_{p,q}\to 0$ 即可. 因为 $\frac{|s-s_0|}{\mathrm{Re}(s-s_0)}$ 在半平面 $\mathrm{Re}(s-s_0)\geqslant 0$ 的扇形 $|\arg(s-s_0)|\leqslant\alpha<\frac{\pi}{2}$ 上被 $\tan\alpha$ 控制, 并且由于在此半平面上 $p^{-\mathrm{Re}(s-s_0)}\leqslant 1$, 由此得到级数 $\sum_{n\geqslant1}a_n n^{-s}$ 在此扇形上满足柯西一致收敛准则, 从而 (ii) 得证. □

推论 VII.1.6. — 设 $L(\boldsymbol{a},s)=\sum_{n\geqslant 1}\frac{a_n}{n^s}$ 是一个狄利克雷级数，而 $\sigma_{\text{conv}}\in\overline{\mathbf{R}}$ 是 $L(\boldsymbol{a},s)$ 的收敛横坐标. 于是 $L(\boldsymbol{a},s)$ 在半平面 $\text{Re}(s)>\sigma_{\text{conv}}$ 中的每一个 s 收敛，并定义了在此半平面上的一个全纯函数，从而 $\sigma_{\text{hol}}\leqslant\sigma_{\text{conv}}$.

证明　由 σ_{conv} 的定义知，对于任意的 $\varepsilon>0$，存在 $s_\varepsilon\in\mathbf{C}$，使得 $L(\boldsymbol{a},s_\varepsilon)$ 收敛，并且 $\text{Re}(s_\varepsilon)\leqslant\sigma_{\text{conv}}+\varepsilon$. 根据定理 VII.1.5，级数 $L(\boldsymbol{a},s)$ 对于半平面 $\text{Re}(s)>\sigma_{\text{conv}}+\varepsilon$ 中的所有 s 均收敛：因为这个半平面是顶点在 s_ε 的扇形的并；由于这个对于所有 $\varepsilon>0$ 都成立，故这证明了 $L(\boldsymbol{a},s)$ 对半平面 $\text{Re}(s)>\sigma_{\text{conv}}$ 中每一个 s 收敛. 而 $L(\boldsymbol{a},s)$ 在此半平面上是全纯的则来自：在所有紧集上全纯函数的一致收敛极限的函数也是全纯的 (定理 V.5.1). □

VII.2. 狄利克雷级数和梅林变换

1. 复平面中的 Γ 函数

欧拉的 Γ 函数是在 $\mathbf{R}_+^*$ 上由公式 $\Gamma(x)=\int_0^{+\infty}e^{-t}t^x\frac{dt}{t}$ 定义的. 我们打算将它推广成整个 $\mathbf{C}$ 平面上的一个亚纯函数. 尽管在习题 V.5.9 中有了另一种处理方式，我们在下面的处理方式则直接地证明 Γ 不化零，从而让我们能推导出余元公式 (习题 VI. 3.19).

回忆：欧拉常数 γ 是 $-\log n+\sum_{k=1}^n\frac{1}{k}$ 当 $n\to+\infty$ 时的极限.

定理 VII.2.1. — (i) 乘积

$$f(z)=ze^{\gamma z}\prod_{k=1}^{+\infty}\Big((1+\frac{z}{k})e^{-z/k}\Big)$$

在 $\mathbf{C}$ 的所有紧集上一致收敛，并在 $\mathbf{R}_+^*$ 上与 $\frac{1}{\Gamma}$ 重合.

(ii) 由 $\Gamma(z)=\frac{1}{f(z)}$ 定义的复 Γ 函数在 $\mathbf{C}$ 上为亚纯的，除了在负整数上为单极点外在其他处均为全纯的，而在 $-n$，其中 $n\in\mathbf{N}$ 的留数为 $\frac{(-1)^n}{n!}$. 又，我们有 $\Gamma(z+1)=z\Gamma(z)$，其中 $z\in\mathbf{C}-(-\mathbf{N})$ 任意.

证明　函数 $h(z)=z^{-2}((1+z)e^{-z}-1)$ 在 $\mathbf{C}$ 上全纯，从而在所有紧集上有界. 特别地，存在 M 使得当 $|z|\leqslant 1$ 时有 $|(1+z)e^{-z}-1|\leqslant M|z^2|$. 现在，如果 K 是一个紧集，则存在 $R(K)$ 使得对所有的 $z\in K$ 有 $|z|\leqslant R(K)$，于是当 $k\geqslant R(K)$ 且 $z\in K$ 时有 $|(1+\frac{z}{k})e^{-z/k}-1|\leqslant\frac{MR(K)^2}{k^2}$. 由此得到在 K 上此乘积的收敛性，那么由定理 V.5.4 知 f 是 C 上的一个全纯函数，并在 0 和 $-k,k\in\mathbf{N}-\{0\}$ 有单零点. 取其倒数则表明 Γ 在 $\mathbf{C}$ 上亚纯，且除在负整数上为单极点外其余均为全纯的. [402]

现在，如果 $x\in\mathbf{R}_+^*$，那么根据高斯公式 (参看习题 IV.1.5) 有

$$\frac{1}{\Gamma(x)}=\lim_{n\to+\infty}\frac{x(x+1)\cdots(x+n)}{n!n^x}=x\lim_{n\to+\infty}e^{-x\log n}\prod_{k=1}^n(1+\frac{x}{k})$$

$$= xe^{\gamma x}\left(\lim_{n\to+\infty} e^{-(1+\cdots+1/n)x}\prod_{k=1}^{n}(1+\frac{x}{k})\right) = xe^{\gamma x}\lim_{n\to+\infty}\prod_{k=1}^{n}\left((1+\frac{x}{k})e^{-x/k}\right),$$

这证明了 f 在 $\mathbf{R}_+^*$ 上与 $\frac{1}{\Gamma}$ 重合.

最后, 函数 $z\mapsto\Gamma(z+1)$ 与 $z\to z\Gamma(z)$ 均在 $\mathbf{C}-(-\mathbf{N})$ 上全纯, 且在 $\mathbf{R}_+^*$ 上重合; 故根据孤立零点定理, 它们在 $\mathbf{C}-(-\mathbf{N})$ 上相等. 由于 $\Gamma(1)=1$, 于是可以对 n 归纳地证明 $\lim_{z\to-n}(z+n)\Gamma(z)=\frac{(-1)^n}{n!}$. 定理证完. □

习题 VII.2.2. — (i) 建立余元公式 $\Gamma(z)\Gamma(1-z)=\frac{\pi}{\sin\pi z}$ (取等号两端的对数导数[5], 并利用习题 V.5.3). 由此给出恒等式 $\int_{-\infty}^{+\infty}e^{-\pi t^2}dt=1$ 的证明.

(ii) 同样, 建立乘法公式: 如果 $p\in\mathbf{N}-\{0\}$ 且 $z\in\mathbf{C}-(-\mathbf{N})$, 则

$$\prod_{j=0}^{p-1}\Gamma(\frac{z+j}{p})=(2\pi)^{(p-1)/2}p^{-z+1/2}\Gamma(z).$$

2. 狄利克雷级数的一个积分公式

变量变换[6] $u=\lambda t$ 表明, 如果 $\lambda\in\mathbf{R}_+^*$, 且 $\mathrm{Re}(s)>0$, 则

$$\frac{1}{\lambda^s}=\frac{1}{\Gamma(s)}\int_0^{+\infty}e^{-\lambda t}t^s\frac{dt}{t}.$$

这个简单的注解对于研究某些狄利克雷级数的解析延拓是非常有用的.

下面总设 $L(\boldsymbol{a},s)=\sum_{n\geqslant1}\frac{a_n}{n^s}$ 是一个在某处收敛的狄利克雷级数.

[403] **引理 VII.2.3.** — (i) 整级数 $F_{\boldsymbol{a}}(z)=\sum_{n=1}^{+\infty}a_nz^n$ 的收敛半径至少为 1.

(ii) $f_{\boldsymbol{a}}(t)=F_{\boldsymbol{a}}(e^{-t})$ 在 $\mathbf{R}_+^*$ 属于 $\mathscr{C}^\infty$ 类, 并且它及其导数在无限远处速降.

证明　由假设, 存在 $\tau\in\mathbf{R}$ 使得 $a_n=O(n^\tau)$; 由此得到 (i), 并且在 0 的一个邻域有 $F_{\boldsymbol{a}}(z)=O(|z|)$. 这意味着 $f_{\boldsymbol{a}}$ 在 $\mathbf{R}_+^*$ 属于 $\mathscr{C}^\infty$ 类并在 $+\infty$ 的邻域为 $O(e^{-t})$(从而为速降, 回忆一下: 对于一个函数 $f:\mathbf{R}_+\to\mathbf{C}$, 这表明对于每个 $N\in\mathbf{N}$, 当 $t\to+\infty$ 时有 $t^Nf(t)$ 有界). 转向 $f_{\boldsymbol{a}}$ 的任意阶导数的情形时, 只要观察到 $f_{\boldsymbol{a}}^{(k)}=f_{\boldsymbol{a}^{(k)}}$, 其中 $\boldsymbol{a}^{(k)}=((-n)^ka_n)_{n\in\mathbf{N}}$ 即可. □

引理 VII.2.4. — 如果 $\mathrm{Re}(s)>\sup(\sigma_{\mathrm{abs}},0)$, 则函数 $f_{\boldsymbol{a}}(t)t^{s-1}$ 在 $\mathbf{R}_+^*$ 上可和, 并有

$$L(\boldsymbol{a},s)=\frac{1}{\Gamma(s)}\int_0^{+\infty}f_{\boldsymbol{a}}(t)t^s\frac{dt}{t}.$$

---

[5]一个函数 f 的对数导数是指函数 $\frac{f'}{f}$; 它是 $\log f$ 的导数.

[6]出现测度 $\frac{dt}{t}$ 的一个理由是它在这种类型的变量变换下不变, 这就像 dt 在变量变换 $u=t+a$ 下不变一样. 换而言之, $\frac{dt}{t}$ 是 $\mathbf{R}_+^*$ 的一个哈尔测度.

证明 如果 $\mathrm{Re}(s)=\sigma>\sup(\sigma_{\mathrm{abs}},0)$, 则

$$\int_0^{+\infty}|f_{\boldsymbol{a}}(t)t^{s-1}|dt\leqslant\int_0^{+\infty}\left(\sum_{n=1}^{+\infty}|a_n|e^{-nt}\right)t^\sigma\frac{dt}{t}$$
$$=\sum_{n=1}^{+\infty}|a_n|\int_0^{+\infty}e^{-nt}t^\sigma\frac{dt}{t}=\Gamma(\sigma)\sum_{n=1}^{+\infty}\frac{|a_n|}{n^\sigma}<+\infty,$$

这证明了 $f_{\boldsymbol{a}}(t)t^{s-1}$ 在 $\mathbf{R}_+^*$ 上可和, 从而级数 $\sum_{n=1}^{+\infty}a_ne^{-nt}t^{s-1}$ 在 $L^1(\mathbf{R}_+^*)$ 中收敛于 $f_{\boldsymbol{a}}(t)t^{s-1}$. 因此我们有

$$\int_0^{+\infty}f_{\boldsymbol{a}}(t)t^{s-1}dt=\sum_{n=1}^{+\infty}\int_0^{+\infty}a_ne^{-nt}t^{s-1}dt=\sum_{n=1}^{+\infty}a_n\frac{\Gamma(s)}{n^s}.$$

证完. □

注记 VII.2.5. — (i) 如果 $f:\mathbf{R}_+^*\to\mathbf{C}$, 则函数 $s\mapsto\mathrm{Mel}(f,s)=\int_0^{+\infty}f(t)t^s\frac{dt}{t}$ 是 f 的梅林 (Mellin) 变换. 利用变量变换 $t=e^u$ 可证明, 在竖直直线 $\mathrm{Re}(s)=\sigma$ 上, 在差一个位似变换下, 梅林变换与 $f(e^u)e^{\sigma u}$ 的傅里叶变换重合, 这让我们可以从傅里叶变换的性质得到它的许多的性质.

(ii) 函数 $f_{\boldsymbol{a}}(t)=\sum_{n=1}^{+\infty}a_ne^{-nt}$ 在 $\mathbf{R}_+^*$ 属于 $\mathscr{C}^\infty$ 类, 但却没有任何理由想当然地认为它在 0 必定是非常好的. 事实上, 狄利克雷级数 $\sum_{n=1}^{+\infty}\frac{a_n}{n^s}$ 的解析延拓的性质与 $f_{\boldsymbol{a}}$ 在 0 的正则性紧密相连. 下面的命题 VII.2.6 给出了对此现象的一个解释.

3. 狄利克雷级数的解析延拓 [404]

命题 VII.2.6. — 设 f 是 $\mathbf{R}_+$ 上的 $\mathscr{C}^\infty$ 类函数, 且它和它的所有导数在无限远速降.

(i) 函数 $M(f,s)=\frac{1}{\Gamma(s)}\int_0^{+\infty}f(t)t^s\frac{dt}{t}$ 在 $\mathrm{Re}(s)>0$ 上有定义, 并有到整个 $\mathbf{C}$ 上的解析延拓.[7]

(ii) 如果 $k\in\mathbf{N}$, 则 $M(f,-k)=(-1)^kf^{(k)}(0)$.

证明 在带状区域 $b>\mathrm{Re}(s)>a>0$ 上有 $|f(t)t^{s-1}|\leqslant|f(t)\sup(t^{a-1},t^{b-1})|$. 但是由于 f 在无限远速降并且在 0 的邻域中按假定有 $a>0$, 故 $\int_0^{+\infty}|f(t)\sup(t^{a-1},t^{b-1})|dt<+\infty$. 现在可以应用定理 V.5.7 的条件了. 于是证明了 $M(f,s)$ 在半平面 $\mathrm{Re}(s)>0$ 上全纯.

另外, 分部积分给出当 $\mathrm{Re}(s)>0$ 时有 $M(f,s)=-M(f',s+1)$. 因此, 更一般地, 当 $\mathrm{Re}(s)>0$ 和 $n\in\mathbf{N}$ 时, 我们有 $M(f,s)=(-1)^nM(f^{(n)},s+n)$. 将前面对 f 所做的用于 $f^{(n)}$ 便得到 $(-1)^nM(f^{(n)},s+n)$ 在半平面 $\mathrm{Re}(s)>-n$ 上全纯. 由于这个函数在半平面 $\mathrm{Re}(s)>0$ 上与 $M(f,s)$ 重合, 这证明了 $M(f,s)$ 有一个到半平面 $\mathrm{Re}(s)>-n$ 的全纯延拓, 又由于这对所有 $n\in\mathbf{N}$ 成立, 故 (i) 得证.

[7] 所定义的广义函数 $f\mapsto M(f,s)$ 是阿达马广义函数的有限部分. (ii) 表明, 如果 $k\in\mathbf{N}$, 则 $M(-k)$ 是狄拉克函数在 0 的质量的 k 阶导数.

(ii) 则来自 $M(f,-k)=(-1)^{k+1}M(f^{(k+1)},1)$ 也等于

$$(-1)^{k+1}\int_0^{+\infty} f^{(k+1)}(t)dt=(-1)^{k+1}[f^{(k)}]_0^{+\infty}=(-1)^k f^{(k)}(0).$$

□

推论 VII.2.7. — 如果 $f_{\boldsymbol{a}}$ 在 $\mathbf{R}_+$ 上属于 $\mathscr{C}^\infty$ 类, 则 $L(\boldsymbol{a},s)$ 有到整个 $\mathbf{C}$ 上的全纯延拓. 此外, 如果 $k\in\mathbf{N}$, 则有 $L(\boldsymbol{a},-k)=(-1)^k f_{\boldsymbol{a}}^{(k)}(0)$.

证明 这是引理 VII.2.4 和命题 VII.2.6 的直接推论: 因为 $f_{\boldsymbol{a}}$ 及其所有阶导数在无限远速降 (引理 VII.2.3). □

注记 VII.2.8. — 公式 $L(\boldsymbol{a},-k)=(-1)^k f_{\boldsymbol{a}}^{(k)}(0)$ 表明为了得到发散级数 $\sum_{n\geqslant 1}a_n n^k$ 的和的值与取 $L(\boldsymbol{a},s)$ 在 $-k$ 的值或者当 $x\to 1^-$ 时 $\sum_{n=1}^{+\infty}a_n n^k x^n$ 的极限是一样的.

4. 在一条竖直带中的增大状态

下面的命题 VII.2.11 证明了一个狄利克雷级数的解析延拓在一条竖直的带中有一个合理的性态; 在后面我们将会用到它 (引理 A.3.1). 它的证明利用了斯特林公式.

[405] **命题 VII.2.9.** — 在所有形如 $|\arg(z)|<\alpha,\alpha<\pi$ 的扇形上, 我们在 $|z|=+\infty$ 的邻域中有如下的展开式:

(i) $\frac{\Gamma'(z)}{\Gamma(z)}=\log z-\frac{1}{2z}+O(\frac{1}{z^2})$;

(ii) $\log\Gamma(z)=z\log z-z+\frac12(\log(2\pi)-\log z)+O(\frac1z)$, 其中 $\log\Gamma(z)=\int_{[1,z]}\frac{\Gamma'(w)}{\Gamma(w)}dw$ 是 $\Gamma(z)$ 的对数, 它在这个扇形中全纯, 并在 $z=1$ 上取值 0 (复斯特林公式).

证明 首先从公式 $\frac{\Gamma'(z)}{\Gamma(z)}=-\gamma-\frac1z+\sum_{k=1}^{+\infty}(\frac1k-\frac{1}{z+k})$ 着手, 它来自将 $\frac{1}{\Gamma}$ 定义为一个收敛的乘积 (定理 V.5.4). 如果 $z\notin\mathbf{R}_-$, 则可重写这个公式为下面的形式 (其中 $[t]$ 代表 t 的整数部分, 而 $\{t\}=t-[t]$ 为其分数部分)

$$\begin{aligned}\frac{\Gamma'(z)}{\Gamma(z)}&=-\gamma-\frac1z+\int_1^{+\infty}\left(\frac{1}{[t]}-\frac{1}{z+[t]}\right)dt\\&=-\gamma-\frac1z+\int_1^{+\infty}\left(\frac{1}{[t]}-\frac1t-\frac{1}{z+[t]}+\frac{1}{z+t}\right)dt+\int_1^{+\infty}\left(\frac1t-\frac{1}{z+t}\right)dt\\&=-\gamma-\frac1z+\int_1^{+\infty}\frac{\{t\}}{t[t]}dt-\int_1^{+\infty}\frac{\{t\}}{(z+t)(z+[t])}dt+[\log\frac{t}{z+t}]_1^{+\infty}.\end{aligned}$$

其次 $[\log\frac{t}{z+t}]_1^{+\infty}=\log(z+1)=\log z+\frac1z+O(\frac{1}{z^2})$, 而 $C=\int_1^{+\infty}\frac{\{t\}}{t[t]}dt$ 是一个常数. 可重写 $\int_1^{+\infty}\frac{\{t\}}{(z+t)(z+[t])}dt$ 为

$$\begin{aligned}\int_1^{+\infty}\frac{\{t\}}{(z+t)(z+[t])}dt&=\int_1^{+\infty}\frac{\{t\}}{(z+t)^2}dt+\int_1^{+\infty}\frac{\{t\}^2}{(z+t)^2(z+[t])}dt\\&=\frac{1}{2(z+1)}+\int_1^{+\infty}\frac{\{t\}-\frac12}{(z+t)^2}dt+\int_1^{+\infty}\frac{\{t\}^2}{(z+t)^2(z+[t])}dt,\end{aligned}$$

且由分部积分给出

$$\int_1^{+\infty} \frac{\{t\}-\frac{1}{2}}{(z+t)^2}dt = [\frac{\{t\}^2-\{t\}}{2(z+t)^2}]_1^{+\infty} + \int_1^{+\infty} \frac{\{t\}^2-\{t\}}{(z+t)^3}dt = \int_1^{+\infty} \frac{\{t\}^2-\{t\}}{(z+t)^3}dt.$$

利用囿于下的弱函数: 当 $u \in \mathbf{R}_+$ 和 $|\arg(z)| \leqslant \alpha$ 时有

$$|z+u|^2 \geqslant \frac{1+\cos\alpha}{2}(|z|+u)^2,$$

于是 $\int_1^{+\infty} \frac{\{t\}^2}{(z+t)^2(z+[t])}dt$ 和 $\int_1^{+\infty} \frac{\{t\}^2-\{t\}}{(z+t)^3}dt$ 被囿于上的强函数 $\int_1^2 \frac{1}{(|z|-2)^3}dt + \int_2^{+\infty}(\frac{2}{1+\cos\alpha})^{3/2}\frac{1}{(|z|+t-1)^3}dt$ 所控制. 由此得知这两个积分是 $O(\frac{1}{z^2})$ 的, 并且 $\frac{1}{2(z+1)} - \frac{1}{2z}$ 也是 $O(\frac{1}{z^2})$ 的, 故最后得到

$$\frac{\Gamma'(z)}{\Gamma(z)} = \log z + C - \gamma - \frac{1}{2z} + H(z),$$

其中 H 在扇形 $|\arg(z)| < \alpha$ 上全纯并满足 $|H(z)| \leqslant \frac{A}{|z|^2}$, 这里的 $|z| \geqslant 1$ 而 $A > 0$ 为一适当的常数. 对上式两端积分得到

$$\log\Gamma(z) = [w\log w - w + (C-\gamma)w - \frac{1}{2}\log w]_1^z + \int_1^z H(w)dw.$$

现在, 如果 $z = re^{i\theta}$, 则可将 $\int_1^z$ 写成 $\int_1^R + \int_R^{\mathrm{Re}^{i\theta}} + \int_{\mathrm{Re}^{i\theta}}^{re^{i\theta}}$, 而当 R 趋向 $+\infty$ 时 $\int_1^R H(w)dw$ 趋向一个常数; 又因为 $|H(w)| \leqslant \frac{A}{R^2}$ 以及圆弧的长为 θR, 故 $\int_{\mathbf{R}}^{\mathrm{Re}^{i\theta}} H(w)dw \to 0$, 而 $|\int_{\mathrm{Re}^{i\theta}}^{re^{i\theta}} H(w)dw| \leqslant \int_r^R \frac{A}{u^2}du \leqslant \frac{A}{r} = \frac{A}{|z|}$. 因此存在 $C' \in \mathbf{C}$ 使得在无限远的邻域中有 $\log\Gamma(z) = z\log z - z + (C-\gamma)z - \frac{1}{2}\log z + C' + O(\frac{1}{z})$. 由在 $+\infty$ 的邻域中成立 [406] 的实的斯特林公式

$$\log(\Gamma(x+1)) = x\log x - x + \frac{1}{2}\log(2\pi x) + o(1)$$

便推出了 $C-\gamma = 0$ 和 $C' = \frac{1}{2}\log(2\pi)$, 于是得到命题的证明. □

推论 VII.2.10. — 当 $|\tau|$ 趋向 $+\infty$ 时, 则在所有有限宽的竖直带上一致地有

$$|\Gamma(\sigma+i\tau)| = \sqrt{2\pi}|\tau|^{\sigma-\frac{1}{2}}e^{-\pi|\tau|/2}(1+O(\frac{1}{\tau})).$$

证明 如果 $s = \sigma + i\tau$ 而 $a \leqslant \sigma \leqslant b$, 其中 $a, b \in \mathbf{R}$ 固定, 于是

$$\log s = \log i\tau + \frac{\sigma}{i\tau} + O(\frac{1}{\tau^2}) = \log|\tau| + \frac{i\pi}{2}\cdot\frac{\tau}{|\tau|} + \frac{\sigma}{i\tau} + O(\frac{1}{\tau^2}).$$

利用命题 VII.2.9 的 (ii) 和上面的公式, 由此得到

$$\mathrm{Re}(\log\Gamma(\sigma+i\tau)) = \sigma\log|\tau| - \frac{\pi|\tau|}{2} + \sigma - \sigma - \frac{1}{2}\log|\tau| + \frac{1}{2}\log(2\pi) + O(\frac{1}{\tau}).$$

得证. □

命题 VII.2.11. — 设 f 是 $\mathbf{R}_+$ 上的一个 $\mathscr{C}^\infty$ 类函数, 并且它及其所有导数均在无限远速降. 如果 $a \leqslant b$ 为两个实数, 则对于每一个 $k \in \mathbf{N}$ 存在 $C_{a,b,k}(f)$ 使得

$$|M(f,s)| \leqslant C_{a,b,k}(f)(1+|\tau|)^{-k}e^{\frac{\pi}{2}|\tau|},$$

其中 $s = \sigma + i\tau$ 而 $a \leqslant \sigma \leqslant b$.

证明　选取 $n \in \mathbf{N}$ 使得 $n + a > k + \frac{1}{2}$. 如果 $s = \sigma + i\tau$ 及 $a \leqslant \sigma \leqslant b$, 则

$$|M(f,s)| \leqslant \frac{1}{|\Gamma(s+n)|}\int_0^{+\infty} |f^{(n)}(t)|t^{\sigma+n}\frac{dt}{t} \leqslant \frac{C_n}{|\Gamma(s+n)|},$$

其中 $C_n = \int_0^{+\infty} |f^{(n)}(t)| \sup(t^{a+n}, t^{b+n})\frac{dt}{t}$. 另外, 根据推论 VII.2.10, 存在 $T > 0$ 使得, 当 $s = \sigma + i\tau$ 且 $|\tau| \geqslant T$ 和 $a \leqslant \sigma \leqslant b$ 时有

$$|\Gamma(s+n)|^{-1} \leqslant \frac{2}{\sqrt{2\pi}}(1+|\tau|)^{\frac{1}{2}-\sigma-n}e^{\frac{\pi}{2}|\tau|} \leqslant \frac{2}{\sqrt{2\pi}}(1+|\tau|)^{-k}e^{\frac{\pi}{2}|\tau|}.$$

因此 $(1+|\tau|)^k e^{-\frac{\pi}{2}|\tau|}|M(f,s)|$ 在 $\{s = \sigma + i\tau, |T| \geqslant T, a \leqslant \sigma \leqslant b\}$ 上有界, 并且因为它在带状 $a \leqslant \mathrm{Re}(s) \leqslant b$ 上连续, 故在此整个带上也有界. 得到结论. □

[407] VII.3. 黎曼 ζ 函数

1. 与乘性函数相关的狄利克雷级数

以 $\mathscr{P}$ 记素数的集合.

称从 $\mathbf{N} - \{0\}$ 到 $\mathbf{C}$ 的函数 $n \mapsto a(n)$ 是乘性的是指, $a(1) = 1$ 且对所有互素的 n 和 m 有 $a(nm) = a(n)(m)$; 称其为严格乘性的是指, $a(1) = 1$ 且对任意的 $m, n \geqslant 1$ 有 $a(nm) = a(n)a(m)$. 注意, 一个严格乘性函数是被 $p \in \mathscr{P}$ 的 $a(p)$ 决定的: 因为, 如果 $n = \prod_{i\in I} p_i^{k_i}$ 是 n 的素因子分解, 则有 $a(n) = \prod_{i\in I} a(p_i)^{k_i}$. 另外, 对于一个乘性函数我们需要了解对于 $p \in \mathscr{P}$ 和 $k \geqslant 1$ 时的 $a(p^k)$. 因此有 $a(n) = \prod_{i\in I} a(p_i^{k_i})$.

命题 VII.3.1. — 如果 $n \mapsto a(n)$ 是乘性的, 且若 $L(\boldsymbol{a}, s) = \sum_{n\geqslant 1}\frac{a_n}{n^s}$ 在某处收敛, 则对在半平面 $\mathrm{Re}(s) > \sigma_{\mathrm{abs}}$ 的所有 s 有

(i) 对于任意的 $p \in \mathscr{P}$ 有 $1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots$ 绝对收敛;

(ii) 乘积 $\prod_{p\in\mathscr{P}}(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots)$ 在所有半平面 $\mathrm{Re}(s) > c > \sigma_{\mathrm{abs}}$ 上一致收敛, 且其值为 $L(\boldsymbol{a}, s)$.

证明　设 $c > \sigma_{\mathrm{abs}}$. 如果 $\mathrm{Re}(s) > c$, 则

$$\sum_{p\in\mathscr{P}} |\frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots| \leqslant \sum_{p\in\mathscr{P}} (|\frac{a(p)}{p^s}| + |\frac{a(p^2)}{p^{2s}}| + \cdots) \leqslant \sum_{n=2}^{+\infty} \frac{|a(n)|}{n^c}| < +\infty.$$

利用定理 V.5.4 (更准确说是此定理的 (i) 的证明) 得到了 (i) 和在 $\mathrm{Re}(s) > c$ 上的乘积的一致收敛性.

如果 $X \in \mathbf{R}_+$, 设 $\mathscr{P}(X)$ 为 $\leqslant X$ 的素数的集合, 而 $I(X)$ 为那些素因子均在 $\mathscr{P}(X)$ 中的整数的集合. 如果 $k \in \mathbf{N}$, 令 $I(X,k)$ 表示形如 $\prod_{p\in\mathscr{P}(X)} p^{k_p}, 0 \leqslant k_p \leqslant k$ 的整数的集合. 因此 $I(X,k)$ 是一个有限集. 另外, $n \mapsto a(n)$ 是乘性的使得

$$\prod_{p\in\mathscr{P}(X)} (1 + \frac{a(p)}{p^s} + \cdots + \frac{a(p^k)}{p^{ks}}) = \sum_{n\in I(X,k)} \frac{a(n)}{n^s}.$$

由于所涉及的级数在绝对值上均被可和级数 $\sum_{n\geqslant 1} |\frac{a(n)}{n^s}|$ 控制, 则对这些级数应用控制收敛定理, 并让 k 趋向 $+\infty$ 便证明了

$$\prod_{p\in\mathscr{P}(X)} (1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots) = \sum_{n\in I(X)} \frac{a(n)}{n^s},$$

然后再令 X 趋向 $+\infty$, 便有

$$\prod_{p\in\mathscr{P}} (1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots) = \sum_{n\geqslant 1} \frac{a(n)}{n^s}.$$

这就是我们想要的. □ [408]

注记 VII.3.2. — (i) 称这个乘积的因子 $1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots$ 为函数 $L(\boldsymbol{a}, s)$ 在 p 的欧拉因子, 而公式 $L(\boldsymbol{a}, s) = \prod_{p\in\mathscr{P}}(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots)$ 为 $L(\boldsymbol{a}, s)$ 的欧拉因子乘积分解 (或者欧拉乘积分解).

(ii) 如果 a 是严格乘性的, 则这些欧拉因子由几何级数给出, 从而有 $L(\boldsymbol{a}, s) = \prod_{p\in\mathscr{P}} \frac{1}{1-a(p)p^{-s}}$.

2. ζ 函数的解析延拓

狄利克雷级数 $L(\mathbf{1}, s) = \sum_{n\geqslant 1} \frac{1}{n^s}$ 以 1 为绝对收敛横坐标 (因为它为正系数的故也是收敛横坐标 (推论 VII.1.2)). 又, $n \mapsto 1$ 是严格乘性的; 因此由一般理论得到以下结果 (欧拉, 1737).

命题 VII.3.3. — 如果 $\mathrm{Re}(s) > 1$, 则 $\sum_{n\geqslant 1} \frac{1}{n^s} = \prod_{p\in\mathscr{P}} \frac{1}{1-p^{-s}}$, 并且这个乘积在整个半平面 $\mathrm{Re}(s) > c > 1$ 上一致收敛.

定理 VII.3.4. — 存在唯一的函数 ζ (黎曼 ζ 函数), 它满足

- ζ 是整个 $\mathbf{C}$ 上的亚纯函数, 并除了在 1 是留数为 1 的单极点外是全纯的;
- 如果 $\mathrm{Re}(s) > 1$, 则 $\zeta(s) = L(\mathbf{1}, s)$.

证明　唯一性是解析延拓唯一性 (推论 V.3.7) 的结果. 如果 $f_1(t) = \sum_{n=1}^{+\infty} e^{-nt} =$

$\frac{1}{e^t-1}$, 而 $g(t)=tf_1(t)$, 那么对于任意的 $\mathrm{Re}(s)>1$ 的 s, 根据引理 VII.2.4 有

$$L(\mathbf{1},s)=\frac{1}{\Gamma(s)}\int_0^{+\infty}f_1(t)t^s\frac{dt}{t}=\frac{1}{(s-1)\Gamma(s-1)}\int_0^{+\infty}tf_1(t)t^{s-1}\frac{dt}{t}=\frac{1}{s-1}M(g,s-1).$$

由于 $g(t)$ 在 $\mathbf{R}_+^*$ 上是 $\mathscr{C}^\infty$ 类的, 且在 0 的邻域中全纯 (因此在 $\mathbf{R}_+$ 上为 $\mathscr{C}^\infty$ 类), 而且它与其所有导数在无限远处速降, 故可应用命题 VII.2.6. 由此得到, $M(g,s)$ 有到整个 $\mathbf{C}$ 的解析延拓, 并满足 $M(g,0)=g(0)=1$. 从而得到结果. □

注记 VII.3.5. — 如果 $s>1$ 为实数, 则由命题 VII.3.3 有 $\log\zeta(s)=-\sum_{p\in\mathscr{P}}\log(1-p^{-s})$. 但 $-\log(1-p^{-s})\sim p^{-s}$, 而 ζ 在 $s=1$ 存在一个极点等于说 $\lim_{s\to1^+}\sum_{p\in\mathscr{P}}p^{-s}=+\infty$. 于是得知素数的倒数的和发散 (欧拉 (1737) 的结果); 特别是, 上述定理证明了素数的集合是无限的 (古已证明), 但比起希腊人的证明来它对于素数的分布说得要多一点.

[409] **习题 VII.3.6.** — 设 $\sum_{n=0}^{+\infty}B_n\frac{t^n}{n!}$ 是 $g(t)=\frac{t}{e^t-1}$ 在 0 的泰勒展开式[8],

(i) 计算 $g(t)-g(-t)$. 从而得到当 $k\geqslant1$ 时有 $B_{2k+1}=0$.

(ii) 如果 $n\in\mathbf{N}$, 证明 $\zeta(-n)=(-1)^n\frac{B_{n+1}}{n+1}$. 由此推出 ζ 在负整数上取有理数[9], 而在 <0 的偶数上为 0.

(iii) 证明 $g(z)-\frac{2i\pi}{z-2i\pi}+\frac{2i\pi}{z+2i\pi}$ 在 $D(0,(4\pi)^-)$ 上全纯. 由此推出当 $n\to+\infty$ 时 $\frac{B_{2n}}{(2n)!}$ 和 $\zeta(1-2n)$ 等价.

3. ζ 函数的函数方程

定理 VII.3.7. — (黎曼, 1858) *ζ 函数满足函数方程*[10]

$$\zeta(s)=2\cdot(2\pi)^{s-1}\cdot\Gamma(1-s)\cdot\sin\frac{\pi s}{2}\cdot\zeta(1-s).$$

注记 VII.3.8. — (i) 设 $\xi(s)=\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$. mod 方程 (习题 VII.2.2)

$$\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin\pi s},\ \Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)=2^{1-s}\Gamma\left(\frac{1}{2}\right)\Gamma(s),\ 和\ \Gamma\left(\frac{1}{2}\right)=\sqrt{\pi},$$

可以从 ζ 的函数方程得到 ξ 满足函数方程

$$\xi(s)=\xi(1-s).$$

---

[8] 这些数是被称为伯努利数的有理数, 我们在数学的所有分支中都可发现它. 特别地,

$$B_0=1,B_1=-\frac{1}{2},B_2=\frac{1}{6},B_3=0,B_4=-\frac{1}{30},\ldots,B_{12}=-\frac{691}{2730},\cdots$$

对于一个数序列是否与伯努利数相关的一个几乎可信的判别准则是看该序列头几项是否出现 691.

[9] ζ 函数或更一般的算术几何的 L 函数在整数的值隐藏着大量的算术信息. 库默尔 (Kummer) 是首先发现这个性质的人之一, 这使他 (1852) 证明了, 如果 p 是一个不整除 $\zeta(-1),\zeta(-3),\ldots,\zeta(2-p)$ 的 $\geqslant3$ 的素数, 则方程 $a^p+b^p=c^p$ 没有满足 $abc\neq0$ 的整数解 (即对这样的 p (称之为*正则*) 的费马大定理.). 直到 100 前, 仅有的非正则素数为 37, 59 和 67.

[10] 这个函数方程已由欧拉 (1749) 猜出, 它建立在对 ζ 在整数的计算上.

(ii) ξ 的函数方程也可直接建立 (参看习题 VII.6.6), 但下面的证明的好处在于可以容易地推广到狄利克雷 L 函数. 进一步说, 我们正是将定理 VII.3.7 的形式下的 ζ 的函数方程应用到了素数定理的证明中的 (附录 A).

证明 如果 $c>0$, 令 γ_c 为连接半直线 $(+\infty, c]$, 与顶点为 $c(\pm 1 \pm i)$ 的正方形边的正向, 再连接半直线 $[c,+\infty)$ 得到的闭道 (图 1). 设

$$F_c(s)=\frac{1}{2i\pi}\int_{\gamma_c} f_1(z)(-z)^s\frac{dz}{z},$$

其中 $f_1(z)=\frac{1}{e^z-1}$, 而 $(-z)^s=\exp(s\log(-z))$, 这里所选取的对数分支为使得它的虚部包含在 $-\pi$ 与 π 之间; 特别, 从 $+\infty$ 到 c 时有 $(-z)^s=e^{-i\pi s}z^s$, 而从 c 到 $+\infty$ 时有 $(-1)^s=e^{i\pi s}z^s$(在跑过正方形之后). [410]

证明在于应用留数公式对出现在 $\zeta(1-s)$ 中的 $F_d(s)-F_c(s)$ 进行计算. 函数 $\zeta(s)$ 由 c 趋向 0 得到, 而当 $c\to+\infty$ 取极限则给出了所要的 $\zeta(s)$ 和 $\zeta(1-s)$ 之间的联系.

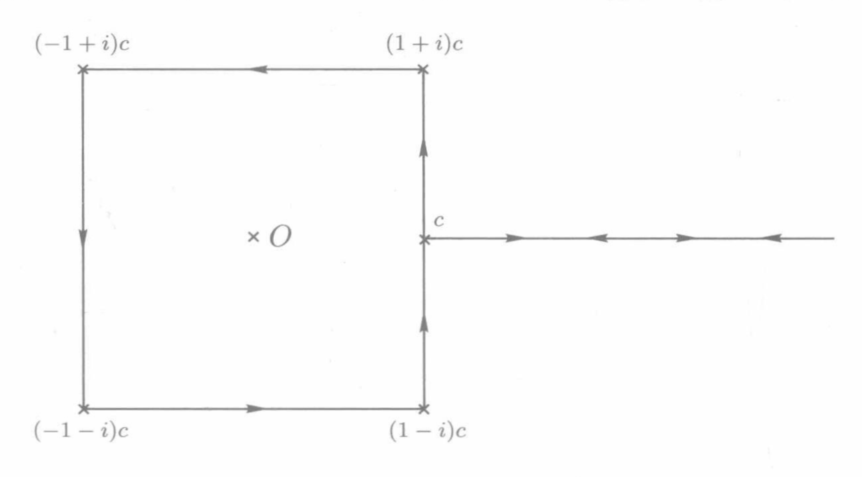


图 1. 道路 γ_c

- $F_d(s)-F_c(s)$ 的计算. (由于对于全纯函数更为熟悉, 这让我们通过以下熟练的技巧去直接证明 $F_d(s)-F_c(s)$ 是函数 $f_1(z)\frac{(-z)^s}{z}$ (它是 $\mathbf{C}-[0,+\infty)$ 上的亚纯函数) 在由 $C_d, [d,c]$ 和按反向前进的 C_c 以及 $[c,d]$ 连接成的道路 $\gamma_{c,d}$ 的内部点的留数和.)

我们进行积分的道路并不真正包含在使被积函数为亚纯的开集中; 为了化成这种情形, 我们必须进行切割分段.

以 g_s^+ (分别地, g_s^-) 表示在由 $\mathbf{C}$ 去掉半直线 $[0,-i\infty)$ (分别地, $[0,+i\infty)$) 得到的开集 Ω^+ (分别地, Ω^-) 上的函数 $f_1(z)\frac{(-z)^s}{z}$, 而所选取的 $\log(-z)$ 的分支是在半直线 $[0,+i\infty)$ 上取实数值的那个. 函数 g_s^+ 和 g_s^- 分别在 Ω^+ 和 Ω^- 上为亚纯的, 并在半平面 $\mathrm{Re}(s)<0$ 上重合; 另外, 在半平面 $\mathrm{Re}(s)>0$ 上 $g_s^-(z)=e^{2i\pi s}g_s^+(z)$.

以 C_c^+(分别地, C_c^-) 表示 C_c 的包含在半平面 $\mathrm{Im}(s)\geqslant 0$ (分别地, $\mathrm{Im}(s)\leqslant 0$) 的分段. 因此有 $C_c^+=[c,(1+i)c]\cdot[(1+i)c,(-1+i)c]\cdot[(-1+i)c,-c]$, 而 $C_c^-=$

$[-c,(-1-i)c]\cdot[(-1-i)c,(1-i)c]\cdot[(1-i)c,c]$. 令 γ_c^+ (分别地, γ_c^-) 为由 $(+\infty,c]$ 与 C_c^+ (分别地, C_c^- 与 $[c,+\infty)$) 连接得到的道路, 并设 $F_c^+(s)=\frac{1}{2i\pi}\int_{\gamma_c^+}g_s^+(z)dz$ 和 $F_c^-(s)=\frac{1}{2i\pi}\int_{\gamma_c^-}g_s^+(z)dz$, 从而使得 $F_c(s)=F_c^+(s)+F_c^-(s)$.

如果 $c<d$, 令 $\gamma_{c,d}^+$ 为闭道 $C_d^+\cdot[-d,-c]\cdot(C_c^+)^{\rm opp}\cdot[c,d]$, 而 $\gamma_{c,d}^-$ 为闭道 $C_d^-\cdot[d,c]\cdot$ [411] $(C_c^-)^{\rm opp}\cdot[-c,-d]$, 其中 $(C_c^+)^{\rm opp}$ 和 $(C_c^-)^{\rm opp}$ 为沿反方向前进的道路 C_c^+ 和 C_c^-). 如我们在下面的图 2 中所看到的, 有

$$F_d^+(s)-F_c^+(s)=\frac{1}{2i\pi}\int_{\gamma_{c,d}^+}g_s^+(z)dz-\frac{1}{2i\pi}\int_{[-d,-c]}g_c^+(z)dz,$$

$$F_d^-(s)-F_c^-(s)=\frac{1}{2i\pi}\int_{\gamma_{c,d}^-}g_s^-(z)dz-\frac{1}{2i\pi}\int_{[-c,-d]}g_c^-(z)dz.$$

由于在 $[-c,-d]$ 上 $g_s^+(z)=g_s^-(z)$, 故上面两个等式相加时它们相互消去, 从而得到

$$F_d(s)-F_c(s)=\frac{1}{2i\pi}\int_{\gamma_{c,d}^+}g_s^-(z)dz+\frac{1}{2i\pi}\int_{\gamma_{c,d}^-}g_s^+(z)dz.$$

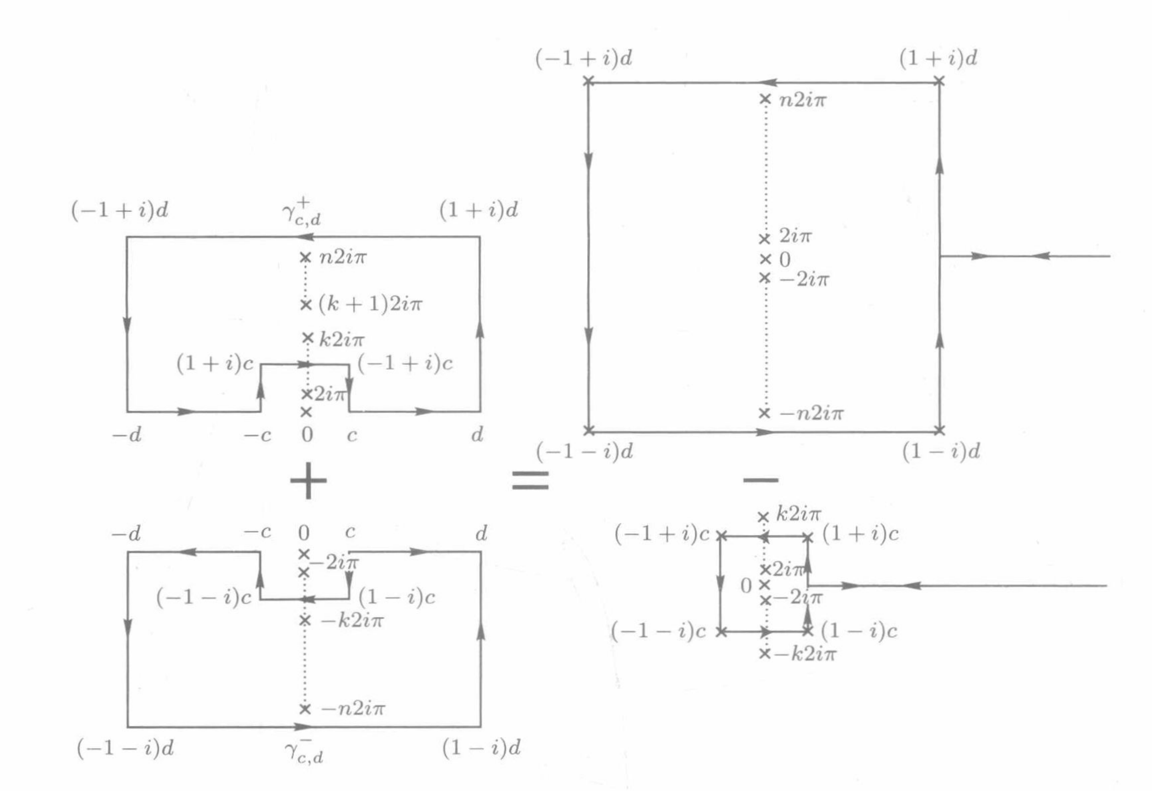


图 2. $\int_{\gamma_d}-\int_{\gamma_c}=\int_{\gamma_{c,d}^+}+\int_{\gamma_{c,d}^-}$

上式右端的项可用留数公式计算. 函数 g_s^+ 在 Ω^+ 上亚纯, 在 $2i\pi k,k\in\mathbf{N}-\{0\}$ 有单极点, 而因为 e^z-1 在 $2i\pi k$ 的导数等于 1, 故有 ${\rm Res}(g_s^+,2i\pi k)=\frac{(-2i\pi k)^s}{2i\pi k}=$

$-(2k\pi)^{s-1}e^{-i\pi\frac{s-1}{2}}$. 同样, g_s^- 在 Ω^- 上亚纯, 在 $-2i\pi k, k\in\mathbf{N}-\{0\}$ 上有单极点, 并有 $\mathrm{Res}(g_s^-,-2i\pi k)=\frac{(2i\pi k)^s}{-2i\pi k}=-(2k\pi)^{s-1}e^{i\pi\frac{s-1}{2}}$. 另外, 当 $c<2k<d$ 时 $\gamma_{c,d}^+$ 相对于 $2i\pi k$ 的指标为 1, 其余情形则为 0. 当 $c<2k<d$ 时 $\gamma_{c,d}^-$ 相对于 $-2i\pi k$ 的指标为 1, 其余情形则为 0. 因此应用留数定理得到

$$F_d(s)-F_c(s)=-\sum_{c<2k\pi<d}2\cos\pi\frac{s-1}{2}\cdot(2k\pi)^{s-1}.$$

• 对 $|(-z)^s|$ 的囿于上的强函数. 我们有 $|(-z)^s|=e^{\mathrm{Re}(s\log(-z))}=|z|^{\mathrm{Re}(s)}e^{-\mathrm{Im}(s)\arg(-z)}$. [412] 由于在所考虑的强函数中 $\arg(-z)$ 在 $-\pi$ 与 π 之间变化, 故证明了, 当 s 固定时, 存在一个常数 $c(s)$ 使得对所有的 z 有 $|(-z)^s|\leqslant c(s)|z|^{\mathrm{Re}(s)}$.

• F_π 与 $\zeta(s)$ 之间的联系. 所得到的对于 $F_d(s)-F_c(s)$ 的公式特别证明了 F_c 在区间 $]0,2\pi[$ 中与 c 无关, 因此 $F_\pi(s)=\lim_{c\to 0^+}F_c(s)$. 然而上面对于 $|(-z)^s|$ 的强函数表明, 当 c 趋向 0 时, C_c 上的积分在 $\mathrm{Re}(s)>1$ 时趋向 0. 因此如果 $\mathrm{Re}(s)>1$, 取极限便得到

$$F_\pi(s)=\frac{1}{2i\pi}\left(e^{-i\pi s}\int_{+\infty}^{0}\frac{1}{e^t-1}t^s\frac{dt}{t}+e^{i\pi s}\int_{0}^{+\infty}\frac{1}{e^t-1}t^s\frac{dt}{t}\right)=\frac{\sin\pi s}{\pi}\cdot\Gamma(s)\cdot\zeta(s).$$

• F_π 与 $\zeta(1-s)$ 之间的联系. 在正方形 $C_{(2N+1)\pi}$ 上有 $|\frac{1}{e^z-1}|\leqslant\frac{1}{1-e^{-(2N+1)\pi}}\leqslant\frac{1}{2}$ (在竖直边界上 $|e^z-1|$ 有囿于下的弱函数 $||e^z|-1|$, 并注意, 在水平边界上 e^z 是负的实数). 利用强控制 $|(-z)^s|\leqslant c(s)|z|^{\mathrm{Re}(s)}$ 得到, 如果 $\mathrm{Re}(s)<0$, 则当 $N\to+\infty$ 时有 $F_{(2N+1)\pi}(s)\to 0$. 在上面对于 $F_d(s)-F_c(s)$ 的公式中取 $d=(2N+1)\pi$, $c=\pi$, 并在 $N\to+\infty$ 时取极限便得到: 如果 $\mathrm{Re}(s)<0$, 则

$$F_\pi(s)=2\cdot\cos\left(\pi\frac{s-1}{2}\right)\cdot(2\pi)^{s-1}\cdot\zeta(1-s).$$

• F_π 的全纯性. 我们有 $F_\pi=\frac{1}{2i\pi}\left(\int_{C_\pi}\frac{(-z)^s}{e^z-1}\frac{dz}{z}+(e^{i\pi s}-e^{-i\pi s})\int_\pi^{+\infty}\frac{t^s}{e^t-1}\frac{dt}{t}\right)$. 如果 $t\in[\pi,+\infty[$, 则在半平面 $\mathrm{Re}(s)>a$ 上有 $|t^s|\leqslant t^a$, 又因为 $\frac{t^{a-1}}{e^t-1}$ 在 $[\pi,+\infty[$ 上可和, 于是由定理 V.5.7 得到 $\int_\pi^{+\infty}\frac{t^s}{e^t-1}\frac{dt}{t}$ 在整个半平面 $\mathrm{Re}(s)>a$ 上对 s 全纯, 从而在整个 $\mathbf{C}$ 上全纯. 而要证明 F_π 在 $\mathbf{C}$ 上全纯, 只需验证 $\int_{C_\pi}\frac{(-z)^s}{e^z-1}\frac{dz}{z}$ 全纯就可以了. 这可以由推论 V.5.8 得到.

• 结论. 由于 $F_\pi,\Gamma,\sin,\cos$ 和 ζ 在整个 $\mathbf{C}$ 上亚纯, 于是利用孤立零点定理, 对于不是上述函数任一个的极点处的 s 有

$$\sin\pi s\cdot\Gamma(s)\cdot\zeta(s)=\pi F_\pi(s)=\cos\pi\frac{s-1}{2}\cdot(2\pi)^s\cdot\zeta(1-s).$$

用公式 $\sin\pi s=-\sin\pi(s-1)=-2\sin\pi\frac{s-1}{2}\cdot\cos\pi\frac{s-1}{2}$, 可以重写这个函数方程为

$$\zeta(1-s)=-2(2\pi)^{-s}\cdot\sin\pi\frac{s-1}{2}\cdot\Gamma(s)\cdot\zeta(s),$$

并将这个函数方程中的 s 换作 $1-s$ 便得到了定理中函数方程的形式. □

习题 VII.3.9. — 以 γ 代表在定理 VII.2.11 中提到的欧拉常数.

(i) 证明 $\Gamma'(1) = -\gamma$.

(ii) 证明, 如果 $\mathrm{Re}(s) > 1$, 则 $\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{+\infty} \int_n^{n+1} (\frac{1}{n^s} - \frac{1}{t^s}) dt$. 由此得到 $\lim_{s\to 1} \zeta(s) - \frac{1}{s-1} = \gamma$, 以及 $\frac{\zeta'(0)}{\zeta(0)} = \log 2\pi$ 和 $\zeta'(0) = -\frac{1}{2}\log 2\pi$.

[413] 4. ζ 函数的零点

定理 VII.3.7 让我们能知道 ζ 函数在复平面上的零点的位置.

推论 VII.3.10. — *ζ 函数的不在竖直带 $0 \leqslant \mathrm{Re}(s) \leqslant 1$ 中仅有的零点是在 < 0 的偶整数上的单零点.*

证明 $\zeta(s)$ 在半平面 $\mathrm{Re}(s) > 1$ 上由绝对收敛的乘积 $\prod_{p\in\mathscr{P}} \frac{1}{1-p^{-s}}$ 给出 (命题 VII. 3.3). 由于此乘积的每个因子在此半平面上不取零值, 故 ζ 在半平面 $\mathrm{Re}(s) > 0$ 上也不取零. 另外, 如果 $\mathrm{Re}(s) < 0$, 则 $\Gamma(1-s) \neq 0$, 按上面所证也有 $\zeta(1-s) \neq 0$. 而定理 VII.3.7 表明 ζ 在半平面 $\mathrm{Re}(s) < 0$ 上的零点与 $\sin \frac{\pi s}{2}$ 的零点相同. 得到结论. □

我们称在负偶整数处的零点为*平凡零点*, 而竖直带 $0 \leqslant \mathrm{Re}(s) \leqslant 1$ 为*临界带*; 这是一个神秘的世界, 在那里什么都很难看得清楚. 上述 ζ 函数的函数方程的证明应归功于黎曼, 在一篇伟大的经典文章中第一次 (在 1858 年) 证明了在此临界带中的零点的分布是如何与素数的分布相关联的 (参看附录 A). 这篇文章也包含了直到今天仍未解决并悬赏一百万美元的*黎曼假设, 即 ζ 在临界带中的零点都在直线 $\mathrm{Re}(s) = \frac{1}{2}$ 上.*

VII.4. 狄利克雷 L 函数

1. 狄利克雷特征标和狄利克雷 L 函数

如果 D 为整数, 一个 mod D 的*狄利克雷特征标*是一个群同态 $\chi : (\mathbf{Z}/D\mathbf{Z})^* \to \mathbf{C}^*$. 狄利克雷特征标的像是 $\mathbf{C}^*$ 的一个有限子群, 因而包含在单位根群之中. 以 $\mathbf{1}_D$ 记*平凡特征标*, 即对于任意的 $a \in (\mathbf{Z}/D\mathbf{Z})^*$, 有 $\mathbf{1}_D(a) = 1$ 的特征标.

如果 χ 是一个 mod D 的狄利克雷特征标, 我们将 $\mathbf{Z}$ 到 $\mathbf{Z}/D\mathbf{Z}$ 的自然投射复合上 χ, 并扩张 χ 使其在与 D 不互素的整数上取 0, 从而常常考虑 χ 为 $\mathbf{Z}$ 上的一个周期为 D 的周期函数. 函数 $\chi \mapsto \chi(n)$ 是严格乘性的: 事实上, 如果 m 和 n 与 D 互素, 则有 mod D 约化的乘性得到 $\chi(mn) = \chi(m)\chi(n)$, 而当 m 或 n 不与 D 互素时 mn 也不与 D 互素, 故 $\chi(mn) = 0 = \chi(m)\chi(n)$. 与 χ 相关的*狄利克雷 L 函数*是指狄利克雷级数 $L(\chi, s) = \sum_{n\geqslant 1} \frac{\chi(n)}{n^s}$. 由于当 $(n, D) = 1$ 时有 $|\chi(n)| = 1$, 故 $L(\chi, s)$ 的绝对收敛横坐标为 1, 从而有下面的命题.

[414] **命题 VII.4.1.** — *设 χ 是个 mod D 狄利克雷特征标.*

(i) *如果 $\mathrm{Re}(s) > 1$, 则 $L(\chi, s) = \prod_{p\in\mathscr{P}} \frac{1}{1-\chi(p)p^{-s}}$, 并且此乘积在每个形如*

$\mathrm{Re}(s) > c > 1$ 的半平面上一致收敛.

(ii) 如果 $\chi \neq \mathbf{1}_D$, 则 $L(\chi, s)$ 的收敛横坐标等于 0.

证明 (i) 完全来自一般理论 (参看命题 VII.3.1). 现在, 如果 $\chi \neq \mathbf{1}_D$, 则存在 $a \in (\mathbf{Z}/D\mathbf{Z})^*$ 使得 $\chi(a) \neq 1$. 于是因为 $x \mapsto ax$ 是 $(\mathbf{Z}/D\mathbf{Z})^*$ 的一个双射, 故有

$$\chi(a) \sum_{x \in (\mathbf{Z}/D\mathbf{Z})^*} \chi(x) = \sum_{x \in (\mathbf{Z}/D\mathbf{Z})^*} \chi(ax) = \sum_{x \in (\mathbf{Z}/D\mathbf{Z})^*} \chi(x).$$

由此得到 $\sum_{x \in (\mathbf{Z}/D\mathbf{Z})^*} \chi(x) = 0$, 从而 $\sum_{n=kD+1}^{(k+1)D} \chi(n) = 0$ (我们也可利用 $(\mathbf{Z}/D\mathbf{Z})^*$ 的特征标 χ 和 $\mathbf{1}_D$ 的正交性). 这表明部分和的序列 $\sum_{k=1}^{n} \chi(k)$ 有界 (绝对值被 D 控制), 因此利用定理 VII.1.5 的 (i) 便证明了 (ii). □

2. 导子与高斯和

如果 D' 是 D 的一个因子, 而 χ 是一个 mod D' 的狄利克雷特征标, 将 χ 与投射 $(\mathbf{Z}/D\mathbf{Z})^* \to (\mathbf{Z}/D'\mathbf{Z})^*$ 复合, 则可将 χ 看作是一个 mod D 的狄利克雷特征标. 称 χ 是本原的是说, 不能找到 D 的因子 D' 使得 χ 是由 mod D' 的特征标经复合得到的. 称 χ 是 D 导子的是说, 它是一个 mod D 的狄利克雷本原特征标. 如果 χ 是 D 导子的, 而 N 是 D 的一个倍数, 则以 χ_N 记由 χ 与投射 $(\mathbf{Z}/N\mathbf{Z})^* \to (\mathbf{Z}/DZ)^*$ 复合得到的 mod N 的狄利克雷特征标.

引理 VII.4.2. — 有 $L(\chi_N, s) = L(\chi, s) \prod_{p|N} (1 - \chi(p)p^{-s})$.

证明 只需利用欧拉的因子的乘积分解即可. □

由于 $1 - \chi(p)p^{-s}$ 在整个 $\mathbf{C}$ 上全纯并且其零点全在直线 $\mathrm{Re}(s) = 0$ 上, 则可看出, 对于狄利克雷 L 函数的解析性质的研究可以化成对与本原特征标相伴的 L 函数的研究.

如果 χ 是一个 mod D 狄利克雷特征标, 以 $\overline{\chi}$ 表示由 $\overline{\chi}(n) = \overline{\chi(n)}$, $n \in (\mathbf{Z}/D\mathbf{Z})^*$ 定义的狄利克雷特征标. 因为 $\chi(n)$ 是一个单位根, 故也有 $\overline{\chi}(n) = \chi(n)^{-1}$.

如果 D 是一个整数, 而 χ 是 D 导子的狄利克雷特征标, 又 $n \in \mathbf{N}$, 那么我们定义扭变高斯和 $G(\chi, n)$ 为

$$G(\chi, n) = \sum_{a \bmod D} \chi(a) e^{2i\pi \frac{na}{D}},$$

并令 $G(\chi) = G(\chi, 1)$.

引理 VII.4.3. — 如果 $n \in \mathbf{N}$, 则 $G(\chi, n) = \overline{\chi}(n) G(\chi)$.

证明 如果 $(n, D) = 1$, 则在 $(\mathbf{Z}/D\mathbf{Z})^*$ 中 n 可逆, 这让我们可写成 [415]

$$G(\chi, n) = \sum_{a \bmod D} \chi(a) e^{2i\pi \frac{na}{D}} = \overline{\chi}(n) \sum_{an \bmod D} \chi(an) e^{2i\pi \frac{na}{D}} = \overline{\chi}(n) G(\chi).$$

如果 $(n, D) = d > 1$, 则可写成 $D = dD'$ 及 $n = dn'$. 由于 χ 是 D 导子的特征标, 故存在 $b \equiv 1 \bmod D/d$ 使得 $\chi(b) \neq 1$ (否则 χ 就会是整除 D' 的导子的特征标). 于是有

$$e^{2i\pi \frac{nab}{D}} = e^{2i\pi \frac{na}{D}} e^{2i\pi \frac{n(b-1)a}{D}} = e^{2i\pi \frac{na}{D}},$$

因为 n 被 d 整除, 而 $b-1$ 被 D/d 整除. 由此得到

$$\chi(b) G(\chi, n) = \sum_{a \bmod D} \chi(ab) e^{2i\pi \frac{nab}{D}} = \sum_{a \bmod D} \chi(a) e^{2i\pi \frac{na}{D}} = G(\chi, n),$$

因此, 由于 $\chi(b) \neq 1$, 故 $G(\chi, n) = 0 = \overline{\chi}(n) G(\chi)$, 证完. □

定理 VII.4.4. — 如果 χ 是导子 $D \neq 1$ 的狄利克雷特征标, 则 $L(\chi, s)$ 具有到整个 $\mathbf{C}$ 的解析延拓. 进一步有 $L(\chi, s) = M(f_\chi, s)$, 其中 $f_\chi : \mathbf{R}_+ \to \mathbf{C}$ 由以下公式给出

$$f_\chi(t) = \frac{1}{G(\overline{\chi})} \sum_{b=1}^{D-1} \frac{\overline{\chi}(b)}{e^{-\frac{2i\pi b}{D}} e^t - 1}.$$

证明　由引理 VII.2.4 得到 $L(\chi, s) = M(f, s)$, 其中 f 由 $f(t) = \sum_{n=1}^{+\infty} \chi(n) e^{-nt}$ 定义. 如果利用引理 VII.4.3 的恒等式[11] $\chi(n) = \frac{G(\overline{\chi}, n)}{G(\overline{\chi})}$, 我们则得到

$$f(t) = \sum_{n=1}^{+\infty} \left(\frac{1}{G(\overline{\chi})} \sum_{b \bmod D} \overline{\chi}(b) e^{2i\pi \frac{nb}{D}} \right) e^{-nt} = \frac{1}{G(\overline{\chi})} \sum_{b=1}^{D-1} \frac{\overline{\chi}(b)}{e^{-\frac{2i\pi b}{D}} e^t - 1} = f_\chi(t).$$

(最后的等式来自: 当 n 是 D 的倍数时 $\chi(n) = 0$, 这使得 $0 \bmod D$ 的数对于此和没有贡献). 现在, f_χ 及其所有导数在无限远处速降, 并且当 $1 \leqslant b \leqslant D-1$ 时有 $e^{2i\pi \frac{nb}{D}} \neq 1$, 故使得 f_χ 在 $\mathbf{R}_+$ 上是 $\mathscr{C}^\infty$ 类的. 利用命题 VII.2.6 便得到结果. □

3. 算术级数的定理

命题 VII.4.5. — $F(s) = \prod_{\chi \in \mathrm{Dir}(D)} L(\chi, s)$[44]是一个系数在 $\mathbf{N}$ 中的狄利克雷级数.

证明　根据命题 VII.4.1, 如果 $\chi \in \mathrm{Dir}(D)$ 且 $\mathrm{Re}(s) > 1$, 则 $L(\chi, s)$ 是 $(1 - \chi(p) p^{-s})^{-1}$ [416] 对于不整除 D 的素数 p 的 (收敛的) 乘积. 因此得到

$$F(s) = \prod_{p \nmid D} \left(\prod_{\chi \in \mathrm{Dir}(D)} (1 - \chi(p) p^{-s})^{-1} \right).$$

现在, $p \mapsto \chi(p)$ 是从 $\mathrm{Dir}(D)$ 到 $\mathbf{C}^*$ 的一个群态射; 它的像是 $\mathbf{C}^*$ 的一个有限子群, 从而具有形式 $\boldsymbol{\mu}_{d(p)}$, 而其核 H_p 是 $\mathrm{Dir}(D)$ 的子群, 以 $h(p)$ 记其基数. 如果 $\eta \in \boldsymbol{\mu}_{d(p)}$,

[11]我们仍然需要验证 $G(\overline{\chi}) \neq 0$(参看习题 VII.4.10).

[44]其中 $\mathrm{Dir}(D)$ 是所有 mod D 狄利克雷特征标的群, 见第 I 章.

则存在 $h(p)$ 个元 $\chi \in \mathrm{Dir}(D)$ 使得 $\chi(p) = \eta$ (如果 χ_0 是其中一个, 则映射 $\chi' \mapsto \chi_0\chi'$ 诱导了从 H_p 到这些 χ 的集合间的一个双射). 由此得到

$$\prod_{\chi\in\mathrm{Dir}(D)} (1-\chi(p)p^{-s}) = \left(\prod_{\eta\in\boldsymbol{\mu}_{d(p)}} (1-\eta p^{-s})\right)^{h(p)},$$

且由于 $\prod_{\eta\in\boldsymbol{\mu}_{d(p)}}(1-\eta X) = 1 - X^{d(p)}$, 故有

$$F(s) = \prod_{p\nmid D}\Big(\frac{1}{1-p^{-d(p)s}}\Big)^{h(p)}.$$

命题的结论来自 $\frac{1}{1-p^{-d(p)s}} = 1 + p^{-d(p)s} + p^{-2d(p)s} + \cdots$ 是一个系数在 $\mathbf{N}$ 中的狄利克雷级数, 而系数在 N 中的狄利克雷级数的乘积仍是一个系数在 $\mathbf{N}$ 中的狄利克雷级数. □

定理 VII.4.6. — (i) $L(\mathbf{1}_D, s)$ 在 $s=1$ 有一个单极点, 且其留数为 $\frac{\varphi(D)}{D}$.

(ii) 如果 $\chi \in \mathrm{Dir}(D) - \{\mathbf{1}_D\}$, 则 $L(\chi, 1) \neq 0$.

证明　考虑到 ζ 在 $s=1$ 有单极点且留数为 1 (定理 VII.3.4), (i) 可由公式 $L(\mathbf{1}_D, s) = \zeta(s)\prod_{p|D}(1-p^{-s})$(参看定理 VII.4.2) 和 $\prod_{p|D}(1-\frac{1}{p}) = \frac{\varphi(D)}{D}$ (小词典的习题 2.9) 得到.

现在, 如果存在 $\chi \in \mathrm{Dir}(D) - \{\mathbf{1}_D\}$ 满足 $L(\chi, 1) = 0$, 则 $L(\chi, s)$ 的零点抵消了 $L(\mathbf{1}_D, s)$ 的单极点; 由此得出 $F(s) = \prod_{\chi\in\mathrm{Dir}(D)} L(\chi, s)$ 在整个 $\mathbf{C}$ 上全纯. 由于根据命题 VII.4.5 知 $F(s)$ 是一个系数在 $\mathbf{N}$ (从而为正) 的狄利克雷级数 $\sum_{n\geqslant 1} a_n n^{-s}$, 那么由兰道定理 (定理 VII.1.1) 级数 $\sum_{n\geqslant 1} a_n n^{-s}$ 对所有的 $s \in \mathbf{C}$ 收敛, 特别 $s=0$ 如此. 因为这些 a_n 属于 $\mathbf{N}$, 这表明它们中只有有限个非零, 这是荒谬的 (因为譬如 $p^{-d(p)s}$ 的系数为 $h(p)$, 并且有无限多个素数).

由此得到 (ii), 证明完成. □

定理 VII.4.7. — (狄利克雷, 1837) 如果 $(a, D) = 1$, 则有无限多个形如 $a + nD$ 的素数, 其中 $n \in \mathbf{N}$.

证明　设 $\phi_a : (\mathbf{Z}/D\mathbf{Z})^* \to \mathbf{C}$ 是一个在 a 取值 1 而其余处取值 0 的函数. 要证明 $\{p, \phi_a(p) = 1\}$ 是一个无限集, 为此, 我们将证明 $\lim_{s\to 1^+} F_a(s) = +\infty$, 其中 $F_a(s) = \sum_p \phi_a(p)p^{-s}$; 这样我们不仅证明了形如 $a + nD$ 的素数的集合无限, 而且也证明了这些素数在整数中十分稠密: 因为它们的倒数的和是发散的 [这个策略是受到 [417] 了欧拉对存在无限多个素数的证明的启发 (注记.VII.3.5)].

从命题 I.2.26 知道, 如果 $p \nmid D$, 则 $\phi_a(p) = \frac{1}{\varphi(D)}\sum_{\chi\in\mathrm{Dir}(D)} \overline{\chi}(a)\chi(p)$, 从而如果 $s > 1$ 为实数, 则有

$$F_a(s) = \frac{1}{\varphi(D)} \sum_{\chi\in\mathrm{Dir}(D)} \overline{\chi}(a) \sum_{p\nmid D} \chi(p)p^{-s}.$$

现在, 当 $p \in \mathscr{P}$ 且 $s>1$ 时有 $|\chi(p)p^{-s}| \leqslant \frac{1}{2}$, 并因为, 如果 $|z| \leqslant \frac{1}{2}$, 则

$$|z+\log(1-z)| \leqslant \frac{|z|^2}{2}+\frac{|z|^3}{3}+\cdots \leqslant \frac{1}{2}\frac{|z|^2}{1-|z|} \leqslant |z|^2.$$

由此得到, 当 $s>1$ 时有

$$|\sum_{p\nmid D}(\chi(p)p^{-s}+\log(1-\chi(p)p^{-s})) \leqslant \sum_{p\nmid D} p^{-2s} \leqslant \zeta(2).$$

函数 $-\sum_{p\nmid D}\log(1-\chi(p)p^{-s})$ 作为一个全纯函数的限制, 在 $]1,+\infty]$ 上连续, 而根据命题 VII.4.1, 它的指数为 $L(\chi,s)$, 故有理由将它写为 $\log L(\chi,s)$. 于是按照上面的控制不等式知 $F_a(s)-\frac{1}{\varphi(D)}\sum_{\chi\in\mathrm{Dir}(D)}\overline{\chi}(a)\log L(\chi,s)$ 当 $s\to 1^+$ 时有界. 然而定理 VII.4.6 的 (ii) 以及 $\log L(\chi,s)$ 在 $s>1$ 的连续性表明 $\sum_{\chi\neq\mathbf{1}_D}\overline{\chi}(a)\log L(\chi,s)$ 在 1^+ 有有限的极限, 而由定理 V.II.4.6 的 (i) 知 $\log L(\mathbf{1}_D,s)$ 在 1^+ 趋向 $+\infty$, 那么, 因为 $\mathbf{1}_D(a)=1$ 故在 1^+, $F_a(s)\to+\infty$, 这就是所要证明的.(利用定理 VII.4.6.(i) 的全部威力可以证明更为准确的结果: $\lim_{s\to 1^+}\frac{F_a(s)}{\log(s-1)}=\frac{1}{\varphi(D)}$.) □

4. 狄利克雷 L 函数的的函数方程

定理 VII.4.8. — 如果 χ 是 $D\neq 1$ 导子的特征标, 则 $L(\chi,s)$ 满足函数方程

$$L(\chi,s)=\begin{cases}2\cdot G(\chi)\cdot D^{-s}\cdot(2\pi)^{s-1}\cdot\Gamma(1-s)\cdot\sin\frac{\pi s}{2}\cdot L(\overline{\chi},1-s), & \text{如果 } \chi(-1)=1,\\ -2i\cdot G(\chi)\cdot D^{-s}\cdot(2\pi)^{s-1}\cdot\Gamma(1-s)\cdot\cos\frac{\pi s}{2}\cdot L(\overline{\chi},1-s), & \text{如果 } \chi(-1)=-1.\end{cases}$$

证明　证明与对 ζ 函数的函数方程的证明极其相似, 因此我们在这里重新采用那里的符号但给出不同的论证. 设 $F_c(\chi,s)=\frac{1}{2i\pi}\int_{\gamma_c}f_\chi(z)(-z)^s\frac{dz}{z}$, 其中 f_χ 是在定理 VII.4.4 中定义的函数. 由于 $f_\chi(z)$ 在无限远处速降, 故函数 $F_c(\chi,s)$ 对于不是形如 $\frac{2\pi b}{D}+2\pi k, k\in\mathbf{N}$ 的 c, 和对于与 D 互素的 $b\leqslant D$ (为了避开 f_χ 的极点) 为全纯的. 因为 f_χ 在顶点 $\frac{2\pi}{D}(\pm 1\pm i)$ 的正方形的内部没有极点, 故对于任意的 $c\in]0,\frac{2\pi}{D}[$ 有 [418] $F_c(\chi,s)=F_{\pi/D}(\chi,s)$. 令 c 趋向 0, 于是, 如果 $\mathrm{Re}(s)>1$ 则有公式

$$F_{\pi/D}=\frac{1}{2i\pi}\left(e^{-i\pi s}\int_{+\infty}^{0}f_\chi(t)t^s\frac{dt}{t}+e^{i\pi s}\int_0^{+\infty}f_\chi(t)t^s\frac{dt}{t}\right)=\frac{\sin\pi s}{\pi}\cdot\Gamma(s)\cdot L(\chi,s).$$

现在, 当 N 趋向 $+\infty$, 则函数 $F_{N\pi}(\chi,s)$ 当 $\mathrm{Re}(s)<0$ 时趋向 0. $F_{\pi/D}(\chi,s)$ 与 $F_{N\pi}(\chi,s)$ 之间的差可由留数定理计算. 而函数 $f_\chi(z)\frac{(-z)^s}{z}$ 在由 $\gamma_{N\pi}$ 和 $\gamma_{\pi/D}$ 之间围成闭道中的 $z=\pm\frac{2i\pi k}{D}$, $1\leqslant k\leqslant ND-1$ 具有极点. 如果 $1\leqslant k\leqslant ND-1$, 则有

$$\mathrm{Res}(f_\chi(z)\frac{(-z)^s}{z},\frac{2i\pi k}{D})=\frac{\overline{\chi}(k)}{G(\overline{\chi})}\frac{(-2i\pi k/D)^s}{(2i\pi k/D)}=-\frac{\overline{\chi}(k)}{G(\overline{\chi})}\cdot\left(\frac{2\pi k}{D}\right)^{s-1}e^{-i\pi\frac{s-1}{2}},$$

$$\mathrm{Res}(f_\chi(z)\frac{(-z)^s}{z},\frac{-2i\pi k}{D})=\frac{\overline{\chi}(-k)}{G(\overline{\chi})}\frac{(2i\pi k/D)^s}{(-2i\pi k/D)}=-\frac{\overline{\chi}(-k)}{G(\overline{\chi})}\cdot\left(\frac{2\pi k}{D}\right)^{s-1}e^{i\pi\frac{s-1}{2}}.$$

因此得到

$$F_{N\pi}(\chi,s)-F_{\pi/D}(\chi,s)=\frac{-1}{G(\overline{\chi})}\sum_{k=1}^{ND-1}(\frac{2\pi k}{D})^{s-1}(\overline{\chi}(k)e^{-i\pi\frac{s-1}{2}}+\overline{\chi}(-k)e^{i\pi\frac{s-1}{2}}).$$

令 N 趋向 $+\infty$, 则当 $\mathrm{Re}(s)<0$ 时得到公式

$$F_{\pi/D}(\chi,s)=\frac{1}{G(\overline{\chi})}\begin{cases}(\frac{2\pi}{D})^{s-1}\cdot(2\cos\pi\frac{s-1}{2})\cdot L(\overline{\chi},1-s), & \text{如果 } \chi(-1)=1,\\ (\frac{2\pi}{D})^{s-1}\cdot(-2i\sin\pi\frac{s-1}{2})\cdot L(\overline{\chi},1-s), & \text{如果 } \chi(-1)=-1.\end{cases}$$

因此从中推出函数方程

$$\sin\pi s\cdot\Gamma(s)\cdot L(\chi,s)=\frac{1}{G(\overline{\chi})}\begin{cases}(2\pi)^s\cdot D^{1-s}\cdot\cos\pi\frac{s-1}{2}\cdot L(\overline{\chi},1-s), & \text{如果 } \chi(-1)=1,\\ -i(2\pi)^sD^{1-s}\cdot\sin\pi\frac{s-1}{2}\cdot L(\overline{\chi},1-s), & \text{如果 } \chi(-1)=-1,\end{cases}$$

也可以将它写成

$$L(\overline{\chi},1-s)=\begin{cases}2G(\overline{\chi})\cdot(2\pi)^{-s}\cdot D^{s-1}\cdot\sin\pi\frac{s-1}{2}\cdot\Gamma(s)\cdot L(\chi,s), & \text{如果 } \chi(-1)=1,\\ -2iG(\overline{\chi})\cdot(2\pi)^{-s}\cdot D^{s-1}\cdot\cos\pi\frac{s-1}{2}\cdot\Gamma(s)\cdot L(\chi,s), & \text{如果 } \chi(-1)=-1.\end{cases}$$

而定理中的函数方程则由将上面的函数方程应用于以 χ 替代 $\overline{\chi}$ 和以 s 替代 $1-s$ 的情形得到. □

注记 VII.4.9. — (i) 如果 χ 是 $D\neq 1$ 导子的狄利克雷特征标, 令

$$w(\chi)=\begin{cases}\dfrac{G(\chi)}{\sqrt{D}}, & \text{如果 } \chi(-1)=1,\\ \dfrac{G(\chi)}{i\sqrt{D}}, & \text{如果 } \chi(-1)=-1,\end{cases}$$

$$\Lambda(\chi,s)=\begin{cases}\Gamma(\dfrac{s}{2})\cdot(\dfrac{D}{\pi})^{s/2}\cdot L(\chi,s), & \text{如果 } \chi(-1)=1,\\ \Gamma(\dfrac{s+1}{2})\cdot(\dfrac{D}{\pi})^{(s+1)/2}\cdot L(\chi,s), & \text{如果 } \chi(-1)=-1.\end{cases}$$

简单的计算可从 $L(\chi,s)$ 的函数方程得到 $\Lambda(\chi,s)$ 满足函数方程 [419]

$$\Lambda(\chi,s)=w(\chi)\Lambda(\overline{\chi},1-s).$$

(ii) 函数 $L(\chi,s)$ 在整个 $\mathbf{C}$ 上全纯, 并在半平面 $\mathrm{Re}(s)>1$ 上不取零值, 而且在此半平面上它由每项均不取零的绝对收敛的乘积给出 (命题 VII.4.1). 它在直线 $\mathrm{Re}(s)=1$ 上不再不取零了 (参看习题 A.4.4), 这是更深刻的结果. 定理 VII.4.8 的函数方程因而证明了在带 $0<\mathrm{Re}(s)<1$ 之外, $L(\chi,s)$ 仅有的零点 (称为平凡的) 当 $\chi(-1)=1$(分别地, $\chi(-1)=-1$) 是在负偶整数 (分别地, 奇数) 上. 人们猜想 (广义黎曼假设, 用英文简记为 GRH) $L(\chi,s)$ 在 $0<\mathrm{Re}(s)<1$ 中的零点位于直线 $\mathrm{Re}(s)=\frac{1}{2}$ 上. 它深刻地涉及在各种算术级数中的素数分布[12].

[12]特别, 涉及在一个算术级数中最小素数的大小, 它自然地涉及许多问题: 例如在密码学中.

习题 VII.4.10. — 设 χ 是 $D \neq 1$ 导子的特征标. 证明

$$\overline{G(\chi)} = \chi(-1)G(\overline{\chi}),\ G(\chi)G(\overline{\chi}) = \chi(-1)D, \quad 以及 \quad |w(\chi)| = 1.$$

习题 VII.4.11. — 考虑将一个整数 n 写成两个平方和的数 $r(n) = |\{(x,y) \in \mathbf{Z}^2, x^2+y^2=n\}|$. 设 $A = \mathbf{Z}[i]$, 且若 $a = x+iy$, 并设[13] $N(a) = x^2+y^2$. 根据习题 A.4.4, 我们有

- $N(ab) = N(a)N(b)$, 其中 $a, b \in A$;
- $A - \{0\}$ 中的任意元 a 具有唯一的分解

$$a = u(1+i)^{k_2} \prod_{p \equiv 1 \bmod 4} q_{p,1}^{k_{p,1}} q_{p,2}^{k_{p,2}} \prod_{p \equiv 3 \bmod 4} p^{k_p},$$

其中 $u \in \{1,-1,i,-i\}$, 而这些 k_p 和 $k_{p,i}$ 是 $\geqslant 0$ 的整数, 同时 $N(q_{p,1}) = N(q_{p,2}) = p$.

(i) 证明, 当 $\mathrm{Re}(s) > 1$ 时有

$$\sum_{n \geqslant 1} \frac{r(n)}{n^s} = \sum_{a \in A-\{0\}} \frac{1}{N(a)^s} = 4\frac{1}{1-2^{-s}} \prod_{p \equiv 1 \bmod 4} \frac{1}{(1-p^{-s})^2} \prod_{p \equiv 3 \bmod 4} \frac{1}{1-p^{-2s}}.$$

$$r(n) = \begin{cases} 0, & \text{如果 } v_p(n) \text{ 对至少一个形如 } 4n+3 \text{ 的素数是奇数,} \\ 4 \displaystyle\prod_{p \equiv 1 \bmod 4} (v_p(n)+1), & \text{如果 } v_p(n) \text{ 对于所有形如 } 4n+3 \text{ 的素数都为偶数.} \end{cases}$$

(ii) 设 $\chi : (\mathbf{Z}/4\mathbf{Z})^* \to \{\pm 1\}$ 为由 $\chi(1) = 1, \chi(-1) = -1$ 定义的狄利克雷特征标. 证明 $\sum_{n \geqslant 1} \frac{r(n)}{n^s} = 4\zeta(s)L(\chi, s)$; 由此推出 $r(n) = 4\sum_{d|n} \chi(d)$.

[420] VII.5. 其他的例子

1. 默比乌斯函数

设 μ 是默比乌斯函数. 它的定义是: 当 n 被至少一个素数的平方整除时 $\mu(n) = 0$, 而当 $n = p_1 \cdots p_r$, 而这些 p_i 互不相同时, $\mu(n) = (-1)^r$. 它是一个乘性函数, 并有

$$\zeta(s)^{-1} = \prod_{p \in \mathscr{P}} (1-p^{-s}) = \sum_{n \in \mathbf{N}} \mu(n) n^{-s} = L(\mu, s).$$

---

[13] 我们有 $N(a) = |A/a|$ (见后文), 在差一个因子 $4 = |A^*|$ 下, 函数 $\sum_{a \in A-\{0\}} \frac{1}{N(a)^s}$ 是出现在附录 G 的前言中的函数 $\zeta_A(s)$. 如果将 $\mathbf{C}$ 与 $\mathbf{R}^2$ 通过 $z = x+iy \mapsto (x,y)$ 等同, 则 A 和 aA 成为了格: A 成为格 $\mathbf{Z}^2$ 体积为 1, 而如果 $a = x+iy$, 则 aA 是以 $a = (x,y)$ 和 $ia = (-y,x)$ 为基的格, 其体积由 a 和 ia 决定, 就是说, $x^2+y^2 = N(a)$. 另外, $(\mathbf{C}/aA)/(A/aA) = \mathbf{C}/A$. 换句话说, 如果 D 是 $\mathbf{C} \bmod A$ 的基本区域, 且如果 S 是 A/aA 的一个代表系, 则这些 $s+D$, $s \in S$ 是两两不交的, 并且它们的并是 $\mathbf{C}/aA$ 的一个基本区域. 因为对于任意的格 Λ, $\mathrm{Vol}(\Lambda)$ 是 Λ 的基本区域的体积, 故由此得到 $|\mathrm{Vol}(aA)| = |A/aA| \cdot \mathrm{Vol}(A)$, 从而 $N(a) = |A/aA|$.

由此得知 $L(\mu,s)$ 可以亚纯延拓到整个复平面. 容易看出它的绝对收敛横坐标 $\sigma_{\text{abs}}=1$, 但它的收敛横坐标 σ_{conv} 却未知. 有人猜想 $\sigma_{\text{conv}}=\frac{1}{2}$, 然而这等价于黎曼假设 (参看 §A.5 的 2 小节).

习题 VII.5.1. — (默比乌斯反演公式)

(i) 证明对于 $n\geqslant 2$ 有 $\sum_{d|n}\mu(d)=0$.

(ii) 设 $F:[0,+\infty[\to \mathbf{C}$ 满足当 $x<1$ 时有 $F(x)=0$, 又设 $G:[0,+\infty[\to \mathbf{C}$ 由 $G(x)=\sum_{n=1}^{+\infty}F(\frac{x}{n})$ 定义. 证明如果 $x<1$ 则 $G(x)=0$, 并且 $F(x)=\sum_{n=1}^{+\infty}\mu(n)G(\frac{x}{n})$.

(iii) 证明当 $x\geqslant 1$ 时有 $\sum_{n=1}^{+\infty}\mu(n)[\frac{x}{n}]=1$.

习题 VII.5.2. — (Báez–Duarte 判别法)

设 E 为 $\phi:[1,+\infty[\to \mathbf{C}$ 使得 $t\mapsto t^{-1}\phi(t)$ 为平方可积的 $\mathscr{L}^2([1,+\infty[,\frac{dt}{t^2})$ 的分离的希尔伯特空间, 其中的范数为 $\langle f,g\rangle=\int_0^{+\infty}\overline{f(t)}g(t)\frac{dt}{t^2}$.

(i) 证明当 $\operatorname{Re}(s)>\frac{1}{2}$ 时有 $t\mapsto t^{1-s}$ 属于 E, 并且对于 ϕ_n 也如此, 其中 $\phi_n(t)=[\frac{t}{n}]-\frac{[t]}{n}$, 而 $n\geqslant 2$ 是一个整数.

(ii) 证明 $\int_1^{+\infty}\{t\}t^{-s-1}dt=\frac{1}{s-1}-\frac{\zeta(s)}{s}$, 其中 $\operatorname{Re}(s)>1$.

(iii) 证明 $s\mapsto\int_1^{+\infty}\{t\}t^{-s-1}dt$ 在半平面 $\operatorname{Re}(s)>0$ 上全纯. 由此得出: 如果 $0<\operatorname{Re}(s)<1$, 则 $\int_0^{+\infty}\{t\}t^{-s-1}dt=-\frac{\zeta(s)}{s}$.

(iv) 证明, 如果 $\operatorname{Re}(s)>\frac{1}{2}$, $n\geqslant 2$, 则 $\langle t^{1-s},\phi_n\rangle=(\frac{1}{n^s}-\frac{1}{n})\frac{\zeta(s)}{s}$.

(v) 由此推出, 如果对于 $n\geqslant 2$, 由 ϕ_n 生成的子空间在 E 中的闭包包含了在 $[1,+\infty[$ 上的常值函数, 则黎曼假设为真[14].

2. 拉马努金函数 τ

拉马努金 (Ramanujan) 函数 τ. 它由恒等式

$$q\prod_{n=1}^{+\infty}(1-q^n)^{24}=\sum_{n=1}^{+\infty}\tau(n)q^n$$

定义. 拉马努金对于这个对象提了两个猜想. 已经被莫德尔 (1917) 证明了的第一个猜想可以叙述为如下形式 [421]

$$L(\tau,s)=\prod_{p\in\mathscr{P}}\frac{1}{1-\tau(p)p^{-s}+p^{11-2s}}.$$

[14] 虽然更加困难, 但我们也可以证明, 如果黎曼假设为真, 则由 $\phi_n, n\geqslant 2$ 生成的子空间的闭包包含了 $[1,+\infty[$ 上的常值函数. 这涉及 Nyman-Beurling (1955) 的一个判别法的一个变化的形式, 即属于 Báez-Duarte (2003) 的一个判别法. 值得注意的是, 习题 VII.5.1 的问题 (iii) 和公式 $\sum_{n=1}^{+\infty}\frac{\mu(n)}{n}=\zeta(1)^{-1}=0$, 让我们证明了当 $t\geqslant 1$ 时有 $\sum_{n=1}^{+\infty}\frac{\mu(n)}{n}\phi_n(t)=-1$, 但是这个级数在 E 中很可能是不收敛的. 级数 $\sum_{n=1}^{+\infty}\frac{\mu(n)}{n}$ 的收敛性比起看起来更加微妙; 它多多少少等价于 ζ 函数在直线 $\operatorname{Re}(s)=1$ 上不取零值.

特别地, τ 是一个乘性函数! 它的证明所基于的事实是, 如果 $q = e^{2i\pi z}$, 则 $z \mapsto \Delta(z) = q\prod_{n=1}^{+\infty}(1-q^n)^{24}$ 是一个对于 $\mathbf{SL}_2(\mathbf{Z})$ 的权为 12 的模形式 (参看习题 VII.6.3 和 VII. 6.11).

拉马努金的第二个猜想断言函数 $L(\tau, s)$ 的欧拉因子在 p 的极点全在直线 $\mathrm{Re}(s) = \frac{11}{2}$ 上. 也可以将它叙述为: 如果 $p \in \mathscr{P}$, 则 $|\tau(p)| \leqslant 2p^{11/2}$. 一直到 1970 年, 德利涅 (P. Deligne) 才证明了这个拉马努金猜想 (在一种称作对任意模形式的拉马努金–皮特森猜想的推广形式下), 它是作为在有限域上簇上的黎曼假设的证明的一个推论得到的, 而后面这个猜想则是韦伊在 1940 年提出来的. 德利涅的证明是格罗滕迪克在 1958 年到 1964 年间所建立的绝对是代数几何的宏伟的革命性纲领的一个顶峰成就.

根据德利涅的结果, $\tau'(p) = \frac{\tau(p)}{2p^{11/2}} \in [-1,1]$, 而产生的问题是这些 $\tau'(p)$ 在此区间中是如何分布的. 佐藤–泰特 (Sato-Tate) 猜想给出了对此问题的答案, 这个猜想的提出可追溯到 1960 年而由哈里斯和泰勒 (Harris-Taylor) 证明 (2009) (借助了 L.Clozel, N. Sheperd-Barron, T. Barnet-Lamb, D. Geraghty ... 的工作). 在拉马努金的 τ 函数的这个特殊情形, 这个猜想断言 $\tau'(p)$ 在测度 $\frac{2\sqrt{1-t^2}}{\pi}dt$ 下在 $[-1,1]$ 中均匀分布: 换句话说, 如果 $-1 \leqslant a \leqslant b \leqslant 1$, 则

$$\lim_{x\to+\infty} \frac{|\{p \leqslant x, a \leqslant \tau'(p) \leqslant b\}|}{|\{p \leqslant x\}|} = \frac{2}{\pi}\int_a^b \sqrt{1-t^2}dt.$$

VII.6. 模形式

随后的一些习题揭示了模形式具有的极为对称的一些性质, 照讲这是不应该存在的, 虽然不是那么显见却真的出现了. 这些性质在非常多的问题中都有所应用 (譬如, 参看第 I 章的脚注 2 和附录 C 的脚注 1). 这里, 我们利用前面各章所得结果证明了一系列漂亮结果, 譬如证明 4 平方和定理 (问题 H.11 提供了证明随后的许多结果的各种方法[15]).

设 $\mathscr{H} = \{z, \mathrm{Im}(z) > 0\}$ 是庞加莱半平面. 回忆 (习题 VI.3.4): 如果 $f: \mathscr{H} \to \mathbf{C}$ 是周期为 1 的全纯周期函数, 则存在一个复数序列 $(a_n(f))_{n\in\mathbf{Z}}$ 使得 $f(z) = \sum_{n\in\mathbf{Z}} a_n(f)e^{2i\pi nz}$, 其中 $z \in \mathscr{H}$ 任意. 令 $e^{2i\pi z} = q$, 并称级数 $\sum_{n\in\mathbf{Z}} a_n(f)q^n$ 为 f 的 q-展开式. 定义 $v_\infty(f) \in \mathbf{Z}\cup\{\pm\infty\}$ 为使得 $a_n(f) \neq 0$ 的 n 的集合的最大下界 (特别, $v_\infty(f) = +\infty$ 当且仅当 $f = 0$).

如果 $k \in \mathbf{Z}$, 一个权为 k 的模函数是 $\mathscr{H}$ 上的一个全纯函数, 它满足:

- 对于任意的 $z \in \mathscr{H}$ 有 $f(z+1) = f(z)$,
- 对于任意的 $z \in \mathscr{H}$ 有 $f(z) = z^{-k}f(-1/z)$,
- $v_\infty(f) > -\infty$.

[15]在解决后面的一系列习题前需先参考问题 H.8 和 H.11: 这些方法十分相似并且也已给出了答案.

如果 $v_\infty(f) \geqslant 0$, 则说 f 是一个权为 k 的模形式, 如果 $v_\infty(f) > 0$, 则说 f 是抛物的 (或者尖点的).

设 Ω 是开集 $\{z \in \mathscr{H}, |z| > 1$, 且 $-\frac{1}{2} < \mathrm{Re}(z) < \frac{1}{2}\}$. 如果 $a, b \in \mathscr{H}$ 满足 [422] $|a| = |b| = 1$, 且若 C^+ 是半径为 1 中心为 0 的包含在 $\mathscr{H}$ 中的半圆, 则以 $A(a,b)$ 记连接 a 和 b 的 C^+ 的圆弧. 令 $\alpha = e^{i\pi/3}$. Ω 的边界 $\partial\Omega$ 于是是竖直半直线 $[\alpha, \alpha + i\infty)$ 和 $[\alpha^2, \alpha^2 + i\infty)$, 以及圆弧 $A(\alpha^2, \alpha)$ 的并. 以 D 表示 Ω, 半直线 $[\alpha, \alpha + i\infty)$ 以及圆弧 $A(i, \alpha)$ 的并.

习题 VII.6.1. — ($\frac{k}{12}$ 公式) 设 f 是一个权为 k 的非零模形式. 本习题的目的是要证明公式

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\alpha(f) + \sum_{z \in D - \{i,\alpha\}} v_z(f) = \frac{k}{12}.$$

(i) 假设 f 在 $\partial\Omega$ 上不取零. 如果 $T \geqslant 2$, 则设 γ_T 为由线段 $[\alpha, \alpha + iT], [\alpha + iT, \alpha^2 + iT], [\alpha^2 + iT, \alpha^2]$ 和圆弧 $A(\alpha^2, \alpha)$ 组成的闭道. 以 $\frac{df}{f}$ 表示 1-形式[16] $\frac{f'(z)}{f(z)}dz$.

- 证明当 $Y \to +\infty$ 时有 $\frac{1}{2i\pi}\int_{[\alpha+iT, \alpha^2+iT]} \frac{df}{f}$ 趋向 $-v_\infty(f)$.
- 证明 $\int_{[\alpha,\alpha+iT]} \frac{df}{f} + \int_{[\alpha^2+iT,\alpha^2]} \frac{df}{f} = 0$.
- 证明 $\int_{A(\alpha^2,i)} \frac{df}{f} = -\int_{A(i,\alpha)} (\frac{df}{f} + \frac{k}{z}dz)$. 由此推出 $\frac{1}{2i\pi}\int_{A(\alpha^2,\alpha)} \frac{df}{f} = \frac{k}{12}$.
- 证明 $v_\infty(f) + \sum_{z\in\Omega} v_z(f) = \frac{k}{12}$.

(ii) 如果不假设 f 在 $\partial\Omega$ 上不取零, 证明有

$$v_\infty(f) + \sum_{z\in\Omega} v_z(f) + \frac{1}{2}\sum_{z\in\partial\Omega-\{\alpha,\alpha^2\}} v_z(f) + \frac{1}{6}(v_\alpha(f) + v_{\alpha^2}(f)) = \frac{k}{12}.$$

(如果 f 在 $z \in \partial\Omega$ 上取零, 则可在 z 的邻域中修改道路 γ_T: 用中心在 z 半径趋向 0 的在 Ω 内部的一段圆弧代替它.)

(iii) 得出结论.

"$\frac{k}{12}$ 公式" 有许多有趣的结果. 这里有几个, 其余的在习题 VII.6.8 和 VII.6.10 中.

习题 VII.6.2. — (模形式空间的维数[17])

(i) 证明一个权为 0 的模形式是常数.

(ii) 证明不存在权为 2 或者为奇数的模形式[18].

(iii) 证明权为 k 的模形式的集合 M_k 是一个向量空间, 且 $f \mapsto (a_n(f))_{0\leqslant n\leqslant \frac{k}{12}}$ 是从 M_k 到 $\mathbf{C}^{d(k)}$ 中的单的线性映射, 其中 $d(k) = 1 + [\frac{k}{12}]$. M_k 为有限维的, 且 $\dim M_k \leqslant 1 + [\frac{k}{12}]$.

---

[16] 注意: 如果 $h = fg$, 则 $\frac{h'}{h} = \frac{f'}{f} + \frac{g'}{g}$, 而当 $h = f \circ \varphi$ 时, 则有 $\frac{h'}{h} = (\frac{f'}{f} \circ \varphi)\varphi'$, 于是应用习题 V.4.5 便可进行计算.

[17] 读者可以在习题 VII.6.12 中找到补充材料.

[18] 这个结果以关键的方式涉及怀尔斯对费马大定理的证明.

习题 VII.6.3. — (模形式的 L 函数)

设 $Y=\{z\in\mathbf{C},\operatorname{Im}(z)\geqslant\frac{1}{2},|\operatorname{Re}(z)|\leqslant\frac{1}{2}\}$. 又设 $f=\sum_{n=1}^{+\infty}a_nq^n$ 是一个权为 $2k$ 的抛物型模形式, 而 $F(z)=\operatorname{Im}(z)^k|f(z)|$.

(i) 证明存在 $M>0$ 使得 $|F(z)|\leqslant M$, 其中 $z\in Y$ 任意.

(ii) 证明 $F(z+1)=F(z)$ 和 $F(-1/z)=F(z)$.

(iii) 证明, 如果 $|\operatorname{Re}(z_0)|\leqslant\frac{1}{2}$ 且 $0<\operatorname{Im}(z_0)\leqslant\frac{1}{2}$, 则存在满足 $|\operatorname{Re}(z_1)\leqslant\frac{1}{2}$, $\operatorname{Im}(z_1)\geqslant 2\operatorname{Im}(z_0)$ 和 $F(z_1)=F(z_0)$ 的 z_1. 由此推出对任意满足 $|\operatorname{Re}(z)|\leqslant\frac{1}{2}$ 的 z, 有 $F(z)\leqslant M$.

[423] (iv) 证明 $a_n=\int_{-1/2}^{1/2}f(x+\frac{i}{n})e^{-2i\pi(nx+i)}dx$. 由此推出 $|a_n|\leqslant e^{2\pi}Mn^k$.

(v) 设 $L(f,s)=\sum_{n=1}^{+\infty}\frac{a_n}{n^s}$. 证明 $L(f,s)$ 具有有限的收敛横坐标, 并具有到整个 $\mathbf{C}$ 的解析延拓, 并证明, 如果 $n\in\mathbf{N}$ 则 $L(f,-n)=0$, 以及 $\Lambda(f,s)=\frac{\Gamma(s)}{(2\pi)^s}L(f,s)$ 满足函数方程 $\Lambda(f,s)=(-1)^k\Lambda(f,2k-s)$. (注意 $\int_0^{+\infty}f(iy)y^s\frac{dy}{y}$.)

在下面的证明中我们将不用空集的理论 (正如每个人所知道的那样, 它的元素具有许多古怪的性质 ⋯⋯).

习题 VII.6.4. — (艾森斯坦 (Eisenstein) 级数)

(i) 证明 $|mz+n|\geqslant\inf(y,\frac{y}{|z|})\sup(|m|,|n|)$, 其中 $z=x+iy\in\mathscr{H}$, 而 $m,n\in\mathbf{Z}$.

(ii) 证明, 如果 $k\geqslant 3$, 则级数 $\sum_{(m,n)\in\mathbf{Z}^2-(0,0)}\frac{1}{(mz+n)^k}$ 在 $\mathscr{H}$ 的每一个紧集上一致收敛.

(iii) 如果 $z\in\mathscr{H}$, 令 $G_k(z)=\frac{\Gamma(k)}{2(-2i\pi)^k}\sum_{(m,n)\in\mathbf{Z}^2-(0,0)}\frac{1}{(mz+n)^k}$. 证明 G_k 是 $\mathscr{H}$ 上的全纯函数, 并且

$$G_k\left(\frac{az+b}{cz+d}\right)=(cz+d)^kG_k(z),$$

其中 $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathbf{SL}_2(\mathbf{Z})$ 为任意.

(iv) 证明: 如果 k 为奇数, 则 $G_k=0$; 而如果 k 为偶数, 则 G_k 是一个非零的权为 k 的模形式.

习题 VII.6.5. — (艾森斯坦级数的 q-展开式)

这个习题的目的是要证明, 如果 $k\geqslant 3$ 是一个偶数, 则 G_k 的 q-展开式由以下公式给出[19]:

$$G_k=\frac{\Gamma(k)}{(-2i\pi)^k}\zeta(k)+\sum_{n=1}^{+\infty}\sigma_{k-1}(n)q^n,\ \text{其中}\ \sigma_{k-1}(n)=\sum_{d|n,d\geqslant 1}d^{k-1}.$$

设 $k\geqslant 2$ 为整数.

[19]我们注意到, 这个 q-展开式除了常数项外的每个项都可清晰看出是有理数. 可以利用这点 (要花点力气) 推出常数项也如此, 这让我们可以给出欧拉关于 ζ 函数在偶整数的值的结果的证明.

(i) 证明级数 $\sum_{n\in\mathbf{Z}}\frac{1}{(z+n)^k}$ 在 $\mathscr{H}$ 的每一个紧集上一致收敛. 由此推出它的和 $A_k(z)$ 是 $\mathscr{H}$ 上的全纯函数.

(ii) 证明 A_k 是周期为 1 的周期函数. 由 (i) 推出 $x\mapsto A_k(x+iy)$ 对于每个 $x\in\mathbf{R}$ 是傅里叶级数 $\sum_{n\in\mathbf{Z}}a_n(y)e^{2i\pi nx}$ 的和.

(iii) 用留数公式计算 $a_n(y)$.

(iv) 由此推出 $\frac{\Gamma(k)}{(-2i\pi)^k}A_k(z)=\sum_{n\geqslant 1}n^{k-1}e^{2i\pi nz}$.

(v) 证明 $G_k(2)=\frac{\Gamma(k)}{(-2i\pi)^k}(\zeta(k)+\sum_{m\geqslant 1}A_k(mz))$, 并由此推出结果.

习题 VII.6.6. — (雅可比 ζ 函数)

(i) 证明 $\theta(z)=\sum_{n\in\mathbf{Z}}e^{i\pi n^2x}$ 在 $\mathscr{H}$ 的每一个紧集上按范数收敛. 由此推出 θ 在 $\mathscr{H}$ 上全纯.

(ii) 利用 $e^{-\pi t^2}$ 的傅里叶变换是 $e^{-\pi x^2}$(参看习题 IV.3.29) 证明 $\theta(iu)=\frac{1}{\sqrt{u}}\theta(\frac{i}{u})$, 其中 $u\in\mathbf{R}_+^*$.

(iii) 由此推出, 当 $z\in\mathscr{H}$ 时有 $\theta(z)=\sqrt{\frac{i}{z}}\theta(\frac{-1}{z})$ (其中 $\sqrt{z}$ 是在 $\mathbf{C}-\mathbf{R}_-$ 上全纯且在 1 取值 1 的 z 的平方根).

(iv) 令 $\xi(s)=\frac{\Gamma(s/2)}{\pi^{s/2}}\zeta(s)$, 其中的 ζ 是黎曼 ζ 函数. 证明, 如果 $\mathrm{Re}(s)>1$, 则 [424] $\xi(s)=\frac{1}{2}\int_0^{+\infty}(\theta(iy)-1)y^{s/2}\frac{dy}{y}$.

(v) 由此推出, 如果 $\mathrm{Re}(s)>1$, 则

$$\xi(s)=-\frac{1}{s}+\frac{1}{s-1}+\frac{1}{2}\int_1^{+\infty}(\theta(iy)-1)(y^{s/2}+y^{(1-s)/2})\frac{dy}{y},$$

然后推出 ξ 具有到 $\mathbf{C}$ 的亚纯延拓, 它在除 $s=0$ 和 $s=1$ 的简单极点外全纯, 并满足函数方程 $\xi(s)=\xi(1-s)$.

(vi) 证明在所有有限宽的竖直带中 $\xi(s)=O(\frac{1}{\mathrm{Im}(s)})$.

习题 VII.6.7. — (权为 2 的艾森斯坦级数)

设 G_2 为 $\mathscr{H}$ 上的周期 1 的全纯周期函数, 其 q-展开式为 [20]

$$G_2=\frac{-1}{24}+\sum_{n=1}^{+\infty}\sigma(n)q^n,\ \text{其中}\ \sigma(n)=\sum_{d|n,d\geqslant 1}d.$$

我们要证明[21] G_2 是几乎模形式的; 准确地说, G_2 满足函数方程 $z^{-2}G_2(-1/z)=G_2(z)-\frac{1}{4i\pi z}$.

---

[20] 如果我们假定有了习题 VII.6.5, 并利用公式 $\zeta(2)=\frac{\pi^2}{6}$, 则可看出 $G_2(s)$ 是这些 $\frac{\Gamma(2)}{(-2i\pi)^2(mz+n)^2}$ 对 n 先求和再对 m 求和得到的.

[21] 这个习题的方法在于从联系 $\Lambda(2-s)$ 和 $\Lambda(s)$ 的函数方程出发, 其中 $\Lambda(s)=\int_0^{+\infty}\varphi(iy)y^s\frac{dy}{y}$, 推导出一个联系 $\varphi(-1/z)$ 和 $\varphi(z)$ 之间的函数方程. 这个方法有许多其他的应用. 例如可以证明其 q-展开式同于 G_k 的展式的函数是一个模形式而无需转向 G_k 的构造和计算它的 q-展开式. 另一个方法在问题 H.11 中给出.

回忆 (习题 VI.3.24): 如果 $y \in \mathbf{R}_+^*$ 及 $c > 0$, 则 $\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\Gamma(s)y^{-s} = e^{-y}$ 绝对收敛.

(i) 证明, 如果 $L(\boldsymbol{a}, s) = \sum_{n=1}^{+\infty}\frac{a_n}{n^s}$ 具有一个有限的收敛横坐标, 则 $F_{\boldsymbol{a}}(z) = \sum_{n=1}^{+\infty} a_n e^{2i\pi nz}$ 在 $\mathbf{C}$ 上全纯, 并且若 $c > \sup(0, \sigma_{\rm abs})$, 于是如果 $y \in \mathbf{R}_+^*$ 则有

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{\Gamma(s)}{(2\pi)^s}L(\boldsymbol{a}, s)y^{-s}ds = F_{\boldsymbol{a}}(iy).$$

(ii) 设 $\sigma(n) = \sum_{d|n, d\geqslant 1} d$. 证明 $L(\sigma, s) = \zeta(s)\zeta(s-1)$.

(iii) 令 $H(s) = \frac{\Gamma(s)}{2\pi)^s}\zeta(s)\zeta(s-1)$. 证明 $H(s) = \frac{s-1}{4\pi}\xi(s)\xi(s-1)$, 由此推出 $H(2-s) = -H(s)$, 和 $H(s)$ 在有限宽的任意竖直带中, 在无限远趋向 0, 以及 H 除在简单极点 0, 1 和 2 外在 $\mathbf{C}$ 上全纯, 而在这些极点的留数分别为 $\frac{1}{24}, \frac{-1}{4\pi}$ 和 $\frac{1}{24}$. (可以利用公式 $\zeta(0) = \frac{-1}{2}, \zeta(-1) = \frac{-1}{12}$ 和 $\zeta(2) = \frac{\pi^2}{6}$.)

(iv) 证明如果 $y > 0$, 则 $G_2(iy) + y^{-2}G_2(i/y) = \frac{1}{24} - \frac{1}{4\pi y} + \frac{1}{24y^2}$.(在顶点为 $3 - iT, 3 + iT, -1 + iT, -1 - iT$ 的矩形上的对 $H(s)y^{-s}$ 积分.)

(v) 结论.

习题 VII.6.8. — 这个习题是为四平方定理做准备. 它的目的是证明如果 $(a_n)_{n\geqslant 2}$ 是一个满足下面条件的复数序列:

- 存在 $c \in \mathbf{N}$ 使得 $a_n = O(n^c)$,
- 如果对于 $z \in \mathscr{H}$, $F(z) = \sum_{n=2}^{+\infty} a_n e^{i\pi nz}$ 满足函数方程 $z^{-4}F(-1/z) = F(z)$,

则对于所有 $n \geqslant 2$ 有 $a_n = 0$.

(i) 证明在 $Y = \{z \in \mathbf{C}, |\mathrm{Re}(z)| \leqslant 1, \mathrm{Im}(z) \geqslant 1\}$ 中有 $F(z) = O(e^{-2\pi \mathrm{Im}(z)})$.

[425] (ii) 证明在 Y 中 $F(1 - \frac{1}{z}) = O(\mathrm{Im}(z)^{c+1})$.

(iii) 设 k 是一个偶整数. 如果 $f : \mathscr{H} \to \mathbf{C}$ 是一个函数, 且如果 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{R})$, 则定义 $f_{|_k}\gamma : \mathscr{H} \to \mathbf{C}$ 为 $f_{|_k}\gamma(z) = (\mathbf{C}z + d)^{-k}f(\frac{az+b}{cz+d})$. 证明这是一个好定义, 并且有 $(f_{|_k}\gamma_1)_{|_k}\gamma_2 = f_{|_k}\gamma_1\gamma_2$, 其中 $\gamma_1, \gamma_2 \in \mathbf{SL}_2(\mathbf{R})$.

(iv) 设 $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, 证明 $S^2 = (TS)^3 = -I$; 由此推出, 对于所有的函数 $f : \mathscr{H} \to \mathbf{C}$ 有 $f_{|_k}S^2 = f_{|_k}(TS)^3 = f$.

(v) 证明 $F_{|_4}TS = F_{|_k}TST$. (关注 $F_{|_4}T^2STSTS^2$ 并计算 $F_{|_4}S$ 和 $F_{|_4}T^2$.)

(vi) 由此推出[22] $F_{|_4}(TS)^2 = F_{|_4}T$ 以及, 如果 $G = F \cdot F_{|_4}TS \cdot F_{|_4}(TS)^2$, 于是在 Y 中有 $G_{|_{12}}S = G_{|_{12}}T = G$, 而 $G = O(\mathrm{Im}(y)^{c+1-4}e^{-4\pi \mathrm{Im}(y)})$.

(vii) 由此推出 G 是一个权为 12 的模形式, 且 $v_\infty(G) \geqslant 2$, 并得结论.

---

[22] 这些结果隐藏在下面的结果中. $\mathbf{SL}_2(\mathbf{R})$ 的由 S 和 T 生成的子群属于 $\mathbf{SL}_2(\mathbf{Z})$, 而由 S 和 T^2 生成的子群是 $\mathbf{SL}_2(\mathbf{Z})$ 中的子群 Γ, 它由那些在 $\mathbf{SL}_2(\mathbf{Z}/2\mathbf{Z})$ 中的像为 I 或 S 的矩阵构成. 由于 $|\mathbf{SL}_2(\mathbf{Z}/2\mathbf{Z})| = 6$, 故 Γ 在 $\mathbf{SL}_2(\mathbf{Z})$ 中的指数为 3, 从而 $I, TS, (TS)^2$ 构成了 $\Gamma \backslash \mathbf{SL}_2(\mathbf{Z})$ 的一个代表系.

习题 VII.6.9. — (四平方和)

本习题的目的是证明下面的公式 (雅可比, 1829), 它是由拉格朗日定理 (1770) 的一个有效形式得到的: *所有的正整数是最多四个平方整数的和*[23]

$$|\{(a,b,c,d)\in \mathbf{Z}^4, a^2+b^2+c^2+d^2=n\}| = 8\sum_{d|n, 4\nmid d} d.$$

以 $r(n)$ 记 $|\{a,b,c,d)\in \mathbf{Z}^4, a^2+b^2+c^2+d^2=n\}|$; 换句话说, $r(n)$ 是 n 分解为四个平方和的个数. 以 $\theta=\sum_{n\in\mathbf{Z}} e^{i\pi n^2 z}$ 记习题 VII.6.6 中的雅可比 θ 函数.

(i) 证明 $\sum_{n=0}^{+\infty} r(n)e^{i\pi nz}=\theta(z)^4$,

(ii) 设 $F(z)=\theta(z)^4-8(G_2(\frac{z}{2})-4G_2(2z))$. 证明 $F_{|_2}S=-F$ 和 $F_{|_2}T^2=F$.(利用习题 VII.6.7.)

(iii) 证明 $r(n)\leqslant(1+2\sqrt{n})^4$ 和 $\sigma(n)\leqslant\frac{n(n+1)}{2}$. 由此推出, 如果 $F(z)=\sum_{n=1}^{+\infty}a_n e^{i\pi nz}$, 则 $a_n=O(n^2)$.

(iv) 由此并利用习题 VII.6.8 推出 $\theta^4(z)=8(G_2(\frac{z}{2})-4G_2(2z))$, 从而得到结论.

因此我们特别有 (因为 $\zeta(4)=\frac{\pi^4}{90},\zeta(6)=\frac{\pi^6}{3^3\cdot5\cdot7}$, 参看习题 V.5.3)

$$G_4=\frac{1}{240}+\sum_{n\geqslant1}\sigma_3(n)q^n,\quad G_6=\frac{-1}{504}+\sum_{n\geqslant1}\sigma_5(n)q^n.$$

于是定义*判别形式* Δ 和*模不变量*[24] j 为

$$\Delta=\frac{1}{1728}((240G_4)^3-(504G_6)^2),\quad j=\frac{(240G_4)^3}{\Delta}.$$

习题 VII.6.10. — (模形式 Δ 和模不变量 j) [426]

(i) 证明 Δ 是一个非零的权为 12 的抛物形式, 并且, 应用 "$\frac{k}{12}$ 公式" 证明 Δ 在 D 上或 $\overline{\Omega}$ 上不取零.

(ii) 证明 j 诱导了从 D 到 $\mathbf{C}$ 的一个双射.

(iii) 证明 G_4 在 D 中仅有的零点是 α, 而 G_6 在 D 中仅有的零点是 i.

(iv) 证明, 如果 $\Delta(z)=0$, 则对任意的 $n\in\mathbf{Z}$ 有 $\Delta(z+n)=0$, 以及 $\Delta(-1/z)=0$. 由此推出, 如果 $\Delta(z_0)=0$ 及 $|\mathrm{Re}(z_0)|\leqslant\frac12$ 和 $|z_0|<1$, 则存在 $z_1\in\mathscr{H}$ 满足 $\Delta(z_1)=0,\mathrm{Im}(z_1)>\mathrm{Im}(z_0)$ 和 $|\mathrm{Re}(z_1)|\leqslant\frac12$.

(v) 证明 Δ 在 $\mathscr{H}$ 上不取零, 而 j 是一个权为 0 的模函数.

习题 VII.6.11. — (Δ 的雅可比公式)

[23] 这个结果已经由 Bachet 和 Méziriac 在 1624 年宣布并由费马在 1638 年推广: 所有的整数是 3 个三角数, 4 个平方数, 5 个五角数, 6 个六角数, 等等之和. (一个数是 k 角数是指形如 $\frac{n((k-2)n-(k-4))}{2}, n\geqslant1$ 的数), 但没有任何证明可寻. 这个推广的断言由柯西在 1815 年证明.

[24] q-展开式 $j=q^{-1}+744+196884q+21493760q^2+\cdots$ 埋藏着许多珍宝 (参看第 I 章脚注 2).

设 $F(q)=q\prod_{n=1}^{+\infty}(1-q^n)^{24}$. 我们的目的是证明 $\Delta(z)=F(e^{2i\pi z})$. 我们将充分地利用习题 VII.6.7 的结果.

(i) 设 $f(z)=\log(F(e^{2i\pi z}))$. 证明 $\frac{1}{2i\pi}f'(z)=-24G_2(z)$.

(ii) 设 $g(z)=f(-1/z)-12\log z$. 证明 $g'(z)=f'(z)$.

(iii) 由此推出, 如果令 $H(z)=F(e^{2i\pi z})$, 则 $\frac{z^{-12}H(-1/z)}{H(z)}$ 在 $\mathscr{H}$ 上为常数, 从而 H 是一个权为 12 的模形式.

(iv) 推出结论.

习题 VII.6.12. — (习题 VII.6.2 的补充)

(i) 证明, 如果 $k\in\{0,4,6,8,10\}$, 则 $\dim M_k=1$. (利用习题 VII.6.5 和 $\frac{k}{12}$ 公式.)

(ii) 证明, 如果 $f=\sum_{n\in\mathbf{N}}a_nq^n\in M_k$ 且 $a_0=0$, 则 $\Delta^{-1}f\in M_{k-12}$.

(iii) 由此推出, 当 $k\equiv 0,4,6,8 \bmod 12$ 时有 $\dim M_k=1+[\frac{k}{12}]$, 而当 $k\equiv 2 \bmod 12$ 时有 $\dim M_k=[\frac{k}{12}]$.

附录 A. 素数定理

A.1. 前言

这一章将致力于证明素数定理和算术级数定理. 自古希腊以来人们已知存在无限多个素数[1]. 它们的分布问题一直吸引着数学家们. 譬如, 这里是欧拉在 1747 年写的一段话: “数学家们一直在寻求发现在素数序列中的某种秩序, 却至今一无所获, 有理由相信, 这是人类智慧永远不能参透的秘密. 如若不信, 请看一看一些人千百年来费了千辛万苦得到的素数表吧: 我们首先意识到的是, 这里既无秩序也无规律. 更加令人惊讶的情形是给予我们具有安全感规则的算术, 以它为工具我们处在可以将这个数的序列延续到所想的地方的境地, 却依然不能让我们感受到哪怕一点点的秩序.”

欧拉自己还有如下的结果:

- 证明了 $\sum_{k=1}^{n}\frac{1}{k}$ 如同 $\log n$ 一样地发散 (等于说 $-\log n+\sum_{k=1}^{n}\frac{1}{k}$ 趋向被称作 “欧拉常数” 的 γ).
- 将 $\sum_{n\in\mathbf{N}}\frac{1}{n}$ 分解为形如 $\prod_{p\in\mathscr{P}}(1+\frac{1}{p}+\frac{1}{p^2}+\cdots)$ 的乘积.
- 注意到这个乘积的对数在差一个收敛和下等于 $\sum\frac{1}{p}$.

在 1737 年, 他给了一个关于素数的无限性的一个新证明 (因为它们的倒数的和发散). 另外, 从公式 $\sum\frac{1}{p}\sim\log(\sum_n\frac{1}{n})$ 出发, 由此得到 $\sum_{p\leqslant x}\frac{1}{p}\sim\log\log x$. 现在, 当 Δx 比起 x 是一个小的数, 则 x 和 $x+\Delta x$ 之间的素数的大小同于 x. 如果以 $\pi(x)$ 记 $\leqslant x$ 的素数的个数, 那么 $\log\log(x+\Delta x)-\log\log x\sim\frac{\pi(x+\Delta x)-\pi(x)}{x}$. 由于 $\log\log x$ 的导数是 $\frac{1}{x\log x}$, 故由此 “推出” 在 x 周围的素数的密度与 $\frac{1}{\log x}$ 同阶, 因 [428]

[1]然而要显式地产生出一个素数不是那么容易的, 迄今已知的最大素数是梅森数 $2^{43112609}-1$, 是在 2008 年 8 月发现的; 写成 10 进位数有 10^7 个字码.

此 $\pi(x) \sim \mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$[2]. 一直等了一个多世纪这个结果才在 1896 年由阿达马 (J. Hadamard) 和普森 (V. Poussin) 独立地给出了证明[3].

定理 A.1.1. — (素数定理) $\pi(x) \sim \frac{x}{\log x}$.

阿达马和普森的证明基于了由黎曼提出的策略, 即利用 ζ 函数的零点与素数分布之间的联系. 基本要素是在欧拉乘积的收敛性不成立的直线 $\mathrm{Re}(s) = 1$ 上不存在 ζ 函数的零点, 而并不能由每个因子不为零之类的得出此结论. 事实上, 素数定理的确等价于 (参看习题 A.4.6) ζ 函数在直线 $\mathrm{Re}(s) = 1$ 上不取零值. 这个等价性让人们长时间认为不可能有一个素数定理的 "初等" (即不利用复变量) 证明, 然而在 1948 年, 爱尔迪希 (Erdös) 和塞尔伯格 (Selberg) 却得到了这样的一个证明, 为此塞尔伯格获得了 1950 年的菲尔兹奖.

如果 P 是一个多项式, 且若没有任何算术的障碍使得 P 在整数上取素数值[4], 则我们可以从一个原则出发, 即 $P(n)$ 在随机取素数与取同样大小的数的机会是一样的, 并设 $\frac{1}{\log P(n)} \sim \frac{1}{\deg P} \cdot \frac{1}{\log n}$. 这是一种直观, 考虑到一个形如 $P(n)$ 的整数被 $p \in \mathscr{P}$ 整除的概率而做的适当修正, 它导致了 Bateman 和 Horn 的下面的猜想.

设 $P_1, \ldots, P_k$ 是整系数的, 在 $\mathbf{Q}[X]$ 中不可约的不同多项式, 且它们的首项系数 > 0; 令 $P = P_1 \cdots P_k$. 如果 $p \in \mathscr{P}$, 则以 $N_p(P)$ 记方程 $P(x) = 0$ 在域 $F_p = \mathbf{Z}/p\mathbf{Z}$ 中解的个数, 并定义常数[5] $C(P) = \prod_{p \in \mathscr{P}}((1 - \frac{1}{p})^{-k}(1 - \frac{N_p(P)}{p}))$.

[429] **猜想 A.1.2.** — (Bateman-Horn, 1962) 如果 $C(P) \neq 0$, 则使得 $P_1(n), \ldots, P_k(n)$ 同时为素数的 $n \in \mathbf{N}$ 的集合为无限集, 并有

$$|\{n \leqslant x, P_1(n) \in \mathscr{P}, \ldots, P_k(n) \in \mathscr{P}\}| \sim \frac{C(P)}{\deg P_1 \cdots \deg P_k} \cdot \frac{x}{(\log x)^k}.$$

素数定理对应于猜想中 $k = 1, P = X$ 的情形. 我们能够确认这个猜想为真的唯一的另一个是 $k = 1$ 而 $P = P_1$ 的次数等于 1 的情形. 在这个情形中, P 具有 $Dx + a$ 形式, 其中 $D \geqslant 2$, 而 a 与 D 互素, 否则就会存在素数 p 使得 $Dx + a \mod p$ 恒等于 0, 从而 $C(P) = 0$. 如果 $p \mid D$, 则 $N_p(P) = 0$, 而如果 $p \nmid D$, 则 $N_p(D) = 1$. Bateman 和 Horn 猜想的常数 $C(P)$ 因此是

$$\prod_{p|D}(1 - \frac{1}{p})^{-1} = \prod_{p|D} \frac{p}{p-1} = \prod_{p|D} \frac{p^{v_p(D)}}{(p-1)p^{v_p(D)-1}} = \frac{D}{\varphi(D)},$$

[2] 函数 $\mathrm{Li}(x)$ 是所谓的对数积分; 在无限远的邻域中我们有 $\mathrm{Li}(x) \sim \frac{x}{\log x}$(进行分部积分: 对 1 积分并对 $\frac{1}{\log t}$ 求导). 于是可以重新叙述素数定理为更有意义的形式: $\pi(x) \sim \frac{x}{\log x}$; 我们正是在这个形式下证明素数定理的, 但 $\mathrm{Li}(x)$ 比起 $\frac{x}{\log x}$ 是对 $\pi(x)$ 更好的近似.

[3] 读者可以验证一下, 如果 $M = \cup_{k \geqslant 1}[2^{2^k}, 2^{2^k+1}[$, 则 $\sum_{n \in \mathbf{N} \cap M, n \leqslant x} \frac{1}{n} \sim \log\log x$, 但 $\frac{|\{n \in \mathbf{N} \cap M, n \leqslant x\}|}{x/\log x}$ 没有极限.

[4] 例如, $12n + 9, n(n^2 + 1)$ 或者 $n(n-1) + 2$ 都显然不能取有限的素数值.

[5] 定义 $C(P)$ 的这个乘积不是收敛的; 我们定义它的值是当 $x \to +\infty$ 时部分和 $\prod_{p \leqslant x}$ 的极限, 这等于说方程 $P(x) = 0$ 的 mod p 的解的个数是 P 在 $\mathbf{Z}[X]$ 中分解为不可约因子乘积的因子的平均个数, 其中假设了 P 在 $\mathbf{Z}[X]$ 无重因子.

其中 $\varphi(D) = |(\mathbf{Z}/D\mathbf{Z})^*|$ 是欧拉指标函数. 因此, Bateman 与 Horn 猜想在这种情形是以下结果的推论 (用 Dx 代替 x).

定理 A.1.3. — (算术级数定理) *如果 $D \geqslant 2$, 而 a 与 D 互素, 并令 $\pi(D,a,x) = |\{p \in \mathscr{P}, p \equiv a \mod D, p \leqslant x\}|$, 则 $\pi(D,a,x) \sim \frac{1}{\varphi(D)} \cdot \frac{x}{\log x}$.*

我们可以重述此定理为: 这些素数如同定理中的形式那样均匀分布在算术级数中; 这个结果属于普森, 如果使用狄利克雷的想法 (1837) 也只对素数定理做了一个小的推广: 狄利克雷 (1837) 已经证明在算术级数中素数均匀分布的结果 (定理 VII.4.7) (相当粗糙, 然而却非常精彩: 譬如, 用手证明了存在形如 $7n+3$ 的素数有无限多个, 这绝非易事 ……). 定理 A.1.3 的证明像证明素数定理那样, 利用了所有的狄利克雷 L 函数 (正是为了证明这个定理才引进的), 以替代仅有的 ζ 函数. 我们已将它转换成了一系列的习题.

算术级数定理也是唯一的我们已知的证明了存在无限多个 n 使得 $P_1(n), \ldots, P_k(n)$ 同时为素数的情形 (这里的 $k=1$). 例如, 我们不知道如何证明存在无限多个 $p \in \mathscr{P}$ 使得 $p+2$ 为素数 (孪生素数问题[6] [45]; 它对应于 $k=2, P_1 = X, P_2 = X+2$). 同样, [430] 我们不知道如何证明存在无限多个形如 n^2+1 的素数[7].

如果可以加进一个变量, 则状况会有很大的改进: 来自动力系统的技术近来已经带来了巨大的进展.

- 2004 年, B. Green 和陶哲轩证明了在素数的集合中存在任意长的算术级数, 这个结果对于陶哲轩得到 2006 年的菲尔兹奖[8] 起了一定的作用. 换言之, 如果 $k \in \mathbf{N}$, 则存在无限多个 $(n_1, n_2) \in \mathbf{N}^2, n_2 \geqslant 1$ 使得 $n_1, n_1+n_2, \ldots, n_1+kn_2 \in \mathscr{P}$.
- 2006 年, 陶哲轩和 T.Ziegler 证明了, 如果 $P_1, \ldots, P_k \in \mathbf{Z}[X]$ 满足 $P_1(0) = \cdots = P_k(0) = 0$, 则存在 $(n_1, n_2) \in \mathbf{N}^2, n_2 \geqslant 1$, 使得 $n_2 + P_1(n_1), \ldots, n_2 + P_k(n_1)$ 都是素数.
- 2010 年, B.Green, 陶哲轩和 T.Ziegler 证明了, 如果 $L_1, \ldots, L_k$ 是 $\mathbf{R}^d, d \geqslant 2$ 上的

---

[6] 一直到 2005 年 D. Goldston 和 C. Yildirim 证明了, 如果以 p_n 表示第 n 个素数, 则 $\liminf \frac{p_{n+1}-p_n}{\log n} = 0$, 这在孪生素数问题的方向上迈出了激励人心的一步 (除以 $\log n$ 的理由是 p_n 的阶是 $n \log n$, 从而 $p_{n+1} - p_n$ 的平均距离为 $\log n$), 陈景润 (1975) 证明了存在无限多个素数 p 使得 $p+2$ 几乎是素数 (即最多是两个素数的乘积).

[7] 自费马以来 (1640 给梅森 (Mersenne de Noël) 的信), 我们知道了所有形如 $4k+1$ 的素数是四个平方和; 由此推出存在无限多个形如 n^2+m^2 的素数, 其中 $n, m \in \mathbf{N}$. 到 1998 年 J. Friedlander 和 Iwaniec 证明了存在无限多个形如 n^2+m^4 的素数; 但这离 n^2+1 还很远, 尽管 Iwaniec 已经证明了 (1978) 存在无限多个 n 使得 n^2+1 几乎是素数 ……

[8] 爱尔迪希曾希望能仅用素数的倒数的和的发散性证明这个结果 (为此他悬赏了 3000 美元). 尽管有相当多的享有盛誉的人以其才智做出了努力 (包括 Roth, Gowers, 布尔盖恩 (Bourgain) 和陶哲轩这四位菲尔兹奖得主), 还是一直不能证明 (或推翻 ……), 如果 $X \subset \mathbf{N} - \{0\}$ 不包含长为 3 的算术级数 (即不存在互不相同的 $a, b, c \in X$ 使得 $a+c=2b$), 则 $\sum_{n \in X} \frac{1}{n} < +\infty$. 在这个方向上最好的是布尔盖恩 (1999) 的一个结果, 它给出 $|\{n \in X, n \leqslant \mathbf{N}\}| \leqslant O(\frac{N\sqrt{\log\log N}}{\sqrt{\log N}})$ (在 2007 年用 $(\log N)^{2/3}$ 替代 $\sqrt{\log N}$ 加以改进, 但应该可以将 2/3 替换成 $1+\delta, \delta > 0$).

[45] 张益唐 (2013) 证明了存在无穷多对素数, 其差小于 7000 万.

整系数的仿射形式 (即 $L_i = L_i' + a_i$, 其中 L_i' 是线性形式, 而 a_i 是常数) 使得 L_i' 两两线性无关 (为了避免, 譬如, $L_1(n) = n_1 + n_2$ 而 $L_2(n) = n_1 + n_2 + 2$ 的情形, 它包含了孪生素数问题), 并且如果

- ◇ $\{n \in \mathbf{N}^d, L_1'(n) > 0, \ldots, L_k'(n) > 0\}$ 非空,
- ◇ $\{n \in \mathbf{N}^d, L_1(n) \cdots L_k(n)\text{不被素数 } p \text{ 整除}\}$ 对于每个 $p \in \mathscr{P}$ 非空,

则存在无限多个 $n = (n_1, \ldots, n_d) \in \mathbf{N}^d$ 使得 $L_1(n), \ldots, L_k(n)$ 是素数. 更准确地说, 如果 $P = L_1 \cdots L_k$, 且若 $N_p(P)$ 是 $P(x) = 0$ 在 $\mathbf{F}_p^d$ 中的解的个数, 则

$$|\{n \in \mathbf{N}^d, \sup_{1 \leqslant i \leqslant d} n_i \leqslant x, L_1(n), \ldots, L_k(n) \in \mathscr{P}\}|$$
$$\sim C_\infty \prod_{p \in \mathscr{P}} \left(\left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{N_p(P)}{p^d}\right) \right) \cdot \frac{x^d}{(\log x)^k},$$

其中 C_∞ 是由 $0 \leqslant t_i \leqslant 1$ 和 $L_i'(t) \geqslant 0$ 定义的凸集的体积 (C_∞ 是使得对所有 i 有 $L_i(n) \geqslant 0$ 的 $n \in \mathbf{N}^d$ 的比例), 而 $\prod_{p \in \mathscr{P}} \left(\left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{N_p(P)}{p^d}\right) \right)$ 是一个收敛的乘积, 这与猜想 A.1.2 的情形相反.

[431] A.2. 函数 ψ 和 ψ_1

1. 素数定理与 ψ_1 在 $+\infty$ 的性态

如果 $(a_n)_{n \in \mathbf{N}}$ 是一个复数序列, 则对于 $\sum_{n \leqslant x} a_n$ 的研究与对狄利克雷级数 $\sum_{n \geqslant 1} a_n n^{-s}$ 的研究如在下面的推论 A.2.5 的证明中那样是有紧密联系的. 为了计算 $\pi(x)$, 自然会引向考虑级数 $\sum_{p \in \mathscr{P}} p^{-s}$, 而它与函数 $-\log \zeta(s)$ 相差得不是很远, 并由于它比起后面这个函数来性质不是太好, 这让我们引进了下面的辅助函数.

- 曼戈尔特 (Mangolt) 函数 Λ 由 $\sum_{n=1}^{+\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}$ 定义. 如果 $\mathrm{Re}(s) > 1$, 则根据命题 VII.3.3 有 $\zeta(s) = \prod_{p \in \mathscr{P}} \frac{1}{1 - p^{-s}}$. 从而当 $\mathrm{Re}(s) > 1$ 时 (定理 V.5.4),

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p \in \mathscr{P}} \frac{p^{-s} \log p}{1 - p^{-s}} = \sum_{p \in \mathscr{P}} \sum_{\nu=1}^{+\infty} \frac{\log p}{p^{\nu s}}.$$

由此推出, 当 n 不是一个素数的幂时 $\Lambda(n) = 0$, 而当 $n = p^\nu, \nu \geqslant 1$ 时 $\Lambda(n) = \log p$.

- 定义函数 ψ 为 $\psi(x) = \sum_{n \leqslant x} \Lambda(n)$.
- 定义函数 ψ_1 为 $\psi_1(x) = \int_0^x \psi(t) dt$.

引理 A.2.1. — 以下的断言在 $+\infty$ 的邻域中等价:

(i) $\pi(x) \sim \frac{x}{\log x}$.

(ii) $\psi(x) \sim x$.

(iii) $\psi_1 \sim \frac{1}{2} x^2$.

证明 按定义, $\psi(x)=\sum_{p^\nu\leqslant x}\log p$. 然而, $p^\nu\leqslant x$ 特别地蕴含了 $\nu\leqslant\frac{\log x}{\log 2}$, 而 $\nu\geqslant 2$ 则表明 $p\leqslant\sqrt{x}$. 由此推出限制不等式

$$\sum_{p\leqslant x}\log p\leqslant\psi(x)\leqslant\sum_{p\leqslant x}\log p+(\sqrt{x}\log x)/\log 2\leqslant\pi(x)\log x+(\sqrt{x}\log x)/\log 2.$$

另外, 如果 $\beta<1$ 且 $x^\beta\leqslant p$, 则有 $\log p\geqslant\beta\log x$. 由此得到

$$\sum_{p\leqslant x}\log p\geqslant\beta\log x((\pi(x)-\pi(x^\beta)),$$

又由于 $\pi(x^\beta)\leqslant x^\beta$, 于是得到, 对于任意的 $\beta<1$, 有限制不等式

$$\beta(\pi(x)\log x-x^\beta\log x)\leqslant\psi(x)\leqslant\pi(x)\log x+(\sqrt{x}\log x)/\log 2.$$

于是得到了 (i) 与 (ii) 的等价性.

蕴含关系 (ii)⇒(iii) 直接由积分得到. 为证明反向的蕴含, 我们注意到 ψ 是一个增函数, 从而

$$\frac{\psi_1(x)-\psi_1((1-\varepsilon)x)}{\varepsilon x}\leqslant\psi(x)\leqslant\frac{\psi_1((1+\varepsilon)x)-\psi_1(x)}{\varepsilon x},$$

其中任意 $\varepsilon>0$. 现在, 如果 $\psi_1(x)=\frac{1}{2}x^2+x^2\eta(x)$, 而 $\lim_{x\to+\infty}\eta(x)=0$, 则对于上面的限制不等式除以 x 便得到下面的限制不等式 [432]

$$1-\frac{\varepsilon}{2}+\frac{\eta(x)-(1-\varepsilon)^2\eta((1-\varepsilon)x)}{\varepsilon}\leqslant\frac{\psi(x)}{x}\leqslant 1+\frac{\varepsilon}{2}+\frac{(1+\varepsilon)^2\eta((1+\varepsilon)x)-\eta(x)}{\varepsilon}.$$

让 x 趋向 $+\infty$, 由此得到 $\liminf\frac{\psi(x)}{x}\geqslant 1-\frac{\varepsilon}{2}$ 和 $\limsup\frac{\psi(x)}{x}\leqslant 1+\frac{\varepsilon}{2}$. 由于这对所有的 $\varepsilon>0$ 成立, 故证明了 $\psi(x)\sim x$, 因此得到结论. □

习题 A.2.2. — 如果 $D\geqslant 2$, 以及 a 与 D 互素, 而 $x\geqslant 1$, 则令

$$\psi(D,a,x)=\sum_{n\leqslant x,n\equiv a\bmod D}\Lambda(n)\quad\text{和}\quad\psi_1(D,a,x)=\int_0^x\psi(D,z,t)dt.$$

证明一下两个断言都等价于算术级数定理"$\varphi(D)\psi(D,a,x)\sim x$"和"$\varphi(D)\psi_1(D,a,x)\sim\frac{x^2}{2}$".

习题 A.2.3. — 证明素数定理等价于 $\text{lcm}(1,\ldots,n)=e^{n+o(n)}$.

2. ψ_1 的积分公式

引理 A.2.4. — 如果 $c>0$ 及 $x>0$, 则

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{x^{s+1}}{s(s+1)}ds=\begin{cases}0, & \text{如果 } x<1,\\ x-1, & \text{如果 } x\geqslant 1.\end{cases}$$

证明 这是一个完全标准的留数计算. 函数 $\frac{x^{s+1}}{s(s+1)}$ 在 $\mathbf{C}$ 上亚纯, 并在两个单极点 $s=0$ 和 $s=-1$ 之外全纯, 而在其上的留数分别为 $\operatorname{Res}(\frac{x^{s+1}}{s(s+1)},0)=x$ 和 $\operatorname{Res}(\frac{x^{s+1}}{s(s+1)},-1)=-1$.

- 如果 $x\geqslant 1$, 令 γ_T 为由线段 $[c-iT,c+iT]$ 和由圆弧 $C^+(T)$ 构成的闭道, 其中的圆弧是 $c+Te^{i\theta},\frac{\pi}{2}\leqslant\theta\leqslant\frac{3\pi}{2}$. 如果 $T>c+1$, 则 γ_T 对于这两个点 0 和 -1 的指标都为 1. 由上面的留数公式得到如果 $T>c+1$ 有 $\frac{1}{2i\pi}\int_{\gamma_T}\frac{x^{s+1}}{s(s+1)}ds=x-1$. 另外, 在 $C^+(T)$ 上有 $|x^{s+1}|\leqslant x^{c+1}$ 以及 $|\frac{1}{s(s+1)}|\leqslant\frac{1}{(T-c)(T-c-1)}$. 因此当 $T\to+\infty$ 时有 $\int_{C^+(T)}\frac{x^{s+1}}{s(s+1)}ds\to 0$ 和

$$\begin{aligned}\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{x^{s+1}}{s(s+1)}ds&=\lim_{T\to+\infty}\frac{1}{2i\pi}\int_{[c-iT,c+iT]}\frac{x^{s+1}}{s(s+1)}ds\\&=x-1-\lim_{T\to+\infty}\int_{C^+(T)}\frac{x^{s+1}}{s(s+1)}ds=x-1.\end{aligned}$$

- 如果 $x<1$, 令 γ_T 为由线段 $[c-iT,c+iT]$ 和圆弧 $C^-(T)$ 构成的闭道, 其中的圆弧是圆 $c+Te^{i\theta}$ 的 θ 在 $\frac{\pi}{2}$ 和 $-\frac{\pi}{2}$ 中的一段. 这时 γ_T 对于两个点 0 和 -1 的指标为 0, 从而留数公式给出 $\frac{1}{2i\pi}\int_{\gamma_T}\frac{x^{s+1}}{s(s+1)}ds=0$, 其中任意 $T>0$. 剩下的推理与上面相同. □

[433] **推论 A.2.5.** — 设 $L(\boldsymbol{a},s)=\sum_{n=1}^{+\infty}\frac{a_n}{n^s}$ 是一个绝对收敛横坐标 $\sigma_{\text{abs}}\neq+\infty$ 的狄利克雷级数. 于是, 如果 $c>\sup(0,\sigma_{\text{abs}})$ 而 $x>0$, 则有

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{L(\boldsymbol{a},s)x^{s+1}}{s(s+1)}ds=\int_0^x\left(\sum_{n\leqslant t}a_n\right)dt.$$

证明 按假设条件, 级数 $\sum_{n=1}^{+\infty}\frac{a_n}{n^s}$ 在直线 $c+i\mathbf{R}$ 上按范数收敛, 又因为函数 $\frac{1}{s(s+1)}$ 在此直线上可和, 故可交换取和与积分. 另外, 我们有

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{1}{n^s}\frac{x^{s+1}}{s(s+1)}ds=\begin{cases}0, & \text{如果 } x<n,\\ n(\frac{x}{n}-1)=x-n, & \text{如果 } x\geqslant n.\end{cases}$$

由此推出

$$\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{L(\boldsymbol{a},s)x^{s+1}}{s(s+1)}ds=\sum_{n\leqslant x}a_n(x-n)=\int_0^x\left(\sum_{n\leqslant t}a_n\right)dt,$$

它给出了结论. □

推论 A.2.6. — 如果 $c>1$ 及 $x>1$, 则

$$\psi_1(x)=-\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{\zeta'(s)}{\zeta(s)}\frac{x^{s+1}}{s(s+1)}ds.$$

习题 A.2.7. — 如果 $D \geqslant 2$, 以 $\mathrm{Dir}(D)$ 记 mod D 的狄利克雷特征标的集合. 我们将利用下面的在 §I.2 的 5 小节中已证明的结果:

$$\text{如果 } a \text{ 与 } D \text{ 互素, 则} \quad \sum_{\chi \in \mathrm{Dir}(D)} \overline{\chi(a)}\chi(n) = \begin{cases} \varphi(D), & \text{如果 } n \equiv a \bmod D, \\ 0, & \text{其他.} \end{cases}$$

那么, 如果 $c > 1$ 而 $x > 1$, 请建立公式

$$\varphi(D)\psi_1(D,a,x) = \frac{1}{2i\pi} \sum_{\chi \in \mathrm{Dir}(D)} \overline{\chi(a)} \int_{c-i\infty}^{c+i\infty} \frac{-L'(\boldsymbol{a},s)}{L(\chi,s)} \frac{x^{s+1}}{s(s+1)} ds.$$

A.3. 显式公式

推论 A.2.6 的公式本身在素数定理的证明中不是十分有用. 我们能从中提取的仅有的信息似乎是, 用直接控制所积分对象的方法, 对所有当 $c > 1$ 时的一个满足 $\psi_1(x) \leqslant C(c)x^{1+c}$ 的常数 $C(c)$ 的存在性, 这从一开始就是清楚的. 为了得到更加精细的结果, 我们将积分的直线移向左边 (以缩小 c 的方式)[9]. 但横穿临界带会带来出现 ζ 的零点的危险, 这会让函数 $\frac{\zeta'}{\zeta}$ 出现许多的极点, 从而函数 $\frac{\zeta'}{\zeta}$ 不能充分小到可以放心地进行移动. 因此我们必须在临界带中控制住函数 $\frac{\zeta'}{\zeta}$, 而全纯函数的奇妙性质 (引理 A.3.6,A.3.9 和 A.3.10) 使得对于从临界带的两条边界上 ζ 函数的知识可以在临界带的内部稍许地控制它 (由于函数方程和斯特林公式, 可以很好掌控在半平面 $\mathrm{Re}(s) < 0$ 上的 ζ 函数). [434]

1. 陈述结果

为了将这一小节的结果应用到 L 函数, 我们将从 $\mathbf{C}$ 上的一个亚纯函数 L 着手, 它在一个在 $s = 1$ 上的可能的极点外全纯, 并满足下面的条件 (L1)—(L3); 这包括了 ζ 函数 (根据引理 A.3.1) 和狄利克雷 L 函数的情形.

(L1) 如果 $a > 1$, 则存在 $c(a)$ 使得, 如果 $\mathrm{Re}(s) \geqslant a$, 则有

$$|L(s)| \leqslant c(a), \ |L(s)^{-1}| \leqslant c(a), \ |\frac{L'(s)}{L(s)}| \leqslant c(a).$$

特别地, L 在半平面 $\mathrm{Re}(s) > 1$ 上不取零.

(L2) 存在 $A \in \mathbf{C}^*, B \in \mathbf{R}_+^*$, 而 $c \in [0, 2[$ 使得 L 满足函数方程

$$L(s) = A \cdot B^s \cdot \Gamma(1-s) \cdot \sin\frac{\pi(s-c)}{2} \cdot \overline{L}(1-s), \text{ 其中 } \overline{L} \text{ 的定义是 } \overline{L}(s) = \overline{L(\overline{s})}.$$

[9] 如果只是对素数定理感兴趣, 那么将积分直线转移向 $-\infty$ 只会造成一点没有什么用处的复杂罢了, 但是却可以建立起素数分布和黎曼 ζ 函数的零点之间的直接联系 (将定理 A.3.3 应用于 $L = \zeta$); 定理 A.3.3 的证明混合着令人愉悦的结果和令人有点沮丧的囿于上的函数; 要了解定理 A.3.3 是如何有用的, 建议读者在看它的证明前去读一下 §A.4.

(L3) 对于任意的实数 $a \leqslant b$, 存在 $C(a,b)>0$ 和 $c(a,b)>0$ 使得, 如果 $a \leqslant \sigma \leqslant b$ 和 $|\tau| \geqslant 1$, 则

$$|L(\sigma+i\tau)| \leqslant C(a,b)e^{c(a,b)|\tau|}.$$

引理 A.3.1. — ζ 函数满足性质 (L1)—(L3).

证明 如果 $\mathrm{Re}(s)>a$, 则有

$$|\zeta(s)| = \prod_{p\in\mathscr{P}} \frac{1}{|1-p^{-s}|} \leqslant \prod_{p\in\mathscr{P}} \frac{1}{1-p^{-\mathrm{Re}(s)}} \leqslant \prod_{p\in\mathscr{P}} \frac{1}{1-p^{-a}} \leqslant \zeta(a),$$

$$|\zeta(s)^{-1}| = \prod_{p\in\mathscr{P}} |1-p^{-s}| \leqslant \prod_{p\in\mathscr{P}} (1+p^{-a}) \leqslant \frac{\zeta(a)}{\zeta(2a)},$$

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \leqslant \sum_{n\in\mathbf{N}} \Lambda(n)|n^{-s}| \leqslant \sum_{n\in\mathbf{N}} \Lambda(n)n^{-a} = \frac{\zeta'(a)}{\zeta(a)},$$

让 $c(a)=\sup(\zeta(a), \frac{\zeta'(a)}{\zeta(a)})$, 则 (L1) 得证. 性质 (L2) 和 (L3) 虽然更加精细但却已经证明过了 (性质 L(2) 是定理 VII.3.7 的对象而命题 VII.2.11(结合上定理 VII.3.4 的证明中的公式 $\zeta(s)=\frac{1}{s-1}M(\frac{t}{e^t-1}, s-1)$ 证明了可以取 $c(a,b)=\frac{\pi}{2}$). □

[435] **习题 A.3.2.** — (i) 证明, 如果 χ 是本原的, 则 $L(\chi,s)$ 满足性质 (L1)—(L3).

(ii) 证明, 如果 χ 是整除 D 的导子的本原特征标, 且 $c>1, x>1$, 则

$$\frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty}\left(\frac{L'(\chi_D,s)}{L(\chi_D,s)}-\frac{L'(\chi,s)}{L(\chi,s)}\right)\frac{x^{s+1}}{s(s+1)}ds = \sum_{p|D}\sum_{\nu\leqslant\frac{\log x}{\log p}}\chi(\nu)(x-p^\nu).$$

由此推出 $\frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty}(\frac{L'(\chi_D,s)}{L(\chi_D,s)}-\frac{L'(\chi,s)}{L(\chi,s)})\frac{x^{s+1}}{s(s+1)}ds$ 是一个 $O(x\log x)$.

设 L 是 $\mathbf{C}$ 上的一个亚纯函数, 在一个在 $s=1$ 上可能的单极点外全纯 (这个可能的单极点实际上可能是某种零点), 并满足性质 (L1)—(L3). 如果 $x>1$, 以 F_x 记函数 $F_x(s)=-\frac{L'(s)}{L(s)}\frac{x^{s+1}}{s(s+1)}$. 这时 $\mathbf{C}$ 上的一个亚纯函数, 并在极点 0 和 -1, 也可能在 1 和 L 的零点外全纯. 由于 L 在 $\mathrm{Re}(s)$ 上不取零并满足函数方程 (L2), L 在带 $0\leqslant \mathrm{Re}(s)\leqslant 1$(临界带) 之外仅有的零点是 $c-2k, k\in\mathbf{N}-\{0\}$, 它可能也包含了 -1. 以 $Y(L)$ 记在临界带中不同于 0 和 1 的零点集合.

设 $a_0=x^{-1}\mathrm{Res}(F_x,0)$, 而 $a_{-1}=\mathrm{Res}(F_x,-1)$[10]. 我们所考虑的结果是下面的"显式公式"(其中的 $v_z(L)\in\mathbf{Z}$ 表示 L 在点 z 的赋值 (即零点的阶)).

定理 A.3.3. — (i) 级数 $\sum_{\rho\in Y(L)}\frac{v_\rho(L)}{\rho(\rho+1)}$ 绝对收敛.

---

[10] 如果 0 不是 L 的零点, 则 $a_0=\frac{-L'(0)}{L(0)}$. 如果 0 是 L 的零点, 则 0 是 F 的二重极点, 从而 a_0 具有 $a_{0,0}+a_{0,1}\log x$ 形式.

如果 $c\neq 1$, 则 -1 是 F 的一个单极点, 从而 $a_{-1}=\frac{L'(1)}{L(1)}$, 如果 $c=1$, 则 -1 是 F 的二重极点, 从而 a_{-1} 具有 $a_{-1,0}+a_{-1,1}\log x$ 形式.

(ii) 如果 $x>1$, 则 $\frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty}\frac{-L'(s)}{L(s)}\frac{x^{s+1}}{s(s+1)}ds$ 也等于

$$-v_1(L)\frac{x^2}{2}+a_0x+a_{-1}-\sum_{\rho\in Y(L)}\frac{v_\rho(L)x^{\rho+1}}{\rho(\rho+1)}-\sum_{k\geqslant 1,c-2k\neq -1}\frac{x^{1+c-2k}}{(2k-c)(2k-c-1)},$$

且上面的这两个级数均绝对收敛.

对它的证明要进行一些准备, 但也应注意到最后的那个表达式可以重写为更加紧凑的形式[11]

$$\frac{1}{2i\pi}\int_{2-i\infty}^{2+i\infty}\frac{-L'(s)}{L(s)}\frac{x^{s+1}}{s(s+1)}ds=\sum_{\mathrm{Re}(\rho)<2}\mathrm{Res}(F_x,\rho),$$

那么定理中的表达式便由 F_x 在它的所有极点上的留数得到 (除了可能是 0 和 1 外均为单极点). 另外, 由于 $|x^{\rho+1}|\leqslant x^3$, 如果 $\mathrm{Re}(\rho)<2$, 则这些级数的收敛性正来自级数 $\sum_{\rho\in Y(L)}\frac{v_\rho(L)}{\rho(\rho+1)}$ 和 $\sum_{k\geqslant 1}\frac{1}{(2k-c)(2k-c-1)}$ 的绝对收敛性. 因此只需证明 (i) 和上面的紧凑形式即可.

2. 在临界带之外的函数 L 和 $\frac{L'}{L}$ [436]

引理 A.3.4. — 如果 $a<0$, 则函数 $(s-a+1)^{a-\frac{3}{2}}(s-1)L(s)$ 在直线 $\mathrm{Re}(s)=a$ 上有界.

证明 在直线 $\mathrm{Re}(s)=a$ 上函数 $F(s)=(s-a+1)^{a-\frac{3}{2}}(s-1)L(s)$ 连续. 另外, 如果 $t\in\mathbf{R}$, 我们有

$$L(a+it)=AB^{a+it}\sin(\frac{\pi(a-c+it)}{2})\Gamma(1-a-it)\overline{L}(1-a-it).$$

然而 $AB^{a+it}\overline{L}(1-a-it)$ 对于 $t\in\mathbf{R}$ 有界, 而 $e^{-\pi|t|/2}|\sin\frac{\pi(a-c+it)}{2}|$ 当 $|t|$ 趋向 $+\infty$ 时趋向 $\frac{1}{2}$, 从而由推论 VII.2.10 得知

$$\left|\sin\left(\frac{\pi(a-c+it)}{2}\right)\Gamma(1-a-it)\right||t|^{-\frac{1}{2}+a}$$

当 $|t|$ 趋向 $+\infty$ 时有界. 因此 $|F(a+it)|=|(it+1)^{a-\frac{3}{2}}(a+it-1)L(a+it)|$ 当 $|t|$ 趋向 $+\infty$ 时有界, 并且由于 $F(a+it)$ 在 $\mathbf{R}$ 上连续, 故它在 $\mathbf{R}$ 上有界. 证完. □

引理 A.3.5. — 设 $(t_n^+)_{n\geqslant 2}$(分别地, $(t_n^-)_{n\geqslant 2}$) 是一个实数序列, 它满足 $n\leqslant t_n^+\leqslant n+1$ (分别地, $-n-1\leqslant t_n^-\leqslant -n$). 令 $b_n^+=-1+it_n^+$ (分别地, $b_n^-=-1+it_n^-$) 以及 $c_n^+=c+1-2n+it_n^+$ (分别地, $c_n^-=c+1-2n+it_n^-$). 于是存在 $C>0$ 使得 $|\frac{L'(s)}{L(s)}|\leqslant C+\log n$, 其中任意 $n\geqslant 2$, 而 $s\in[b_n^+,c_n^+]\cup[c_n^+,c_n^-]\cup[c_n^-,b_n^-]$.

[11]形式上说, 这个公式不外乎就是留数公式, 只需将直线 $\mathrm{Re}(s)=2$ 看成是包围了半平面 $\mathrm{Re}(s)<2$ 的闭道即可.

证明 从函数方程 (L2) 着手, 由它推出恒等式

$$\frac{L'(s)}{L(s)} = \log B + \frac{i\pi}{2} \cdot \frac{e^{i\pi(s-c)/2} + e^{-i\pi(s-c)/2}}{e^{i\pi(s-c)/2} - e^{-i\pi(s-c)/2}} - \frac{\Gamma'(1-s)}{\Gamma(1-s)} - \frac{\overline{L}'(1-s)}{\overline{L}(1-s)}.$$

现在, 当 s 在 $[b_n^+, c_n^+] \cup [c_n^+, c_n^-] \cup [c_n^-, b_n^-]$ 中时我们有 $\mathrm{Re}(1-s) \geqslant 2$.

- 然而如果 $\mathrm{Re}(1-s) \geqslant 2$, 则根据性质 (L1) 有 $|\frac{\overline{L}'(1-s)}{\overline{L}(1-s)}| \leqslant c(2)$.
- 根据命题 VII.2.9, 存在 $C_1 > 0$ 使得当 $\mathrm{Re}(1-s) \geqslant 2$ 时有 $|\frac{\Gamma'(1-s)}{\Gamma(1-s)} - \log(1-s)| \leqslant C_1$. 由此得到, 当 $s \in [b_n^+, c_n^+] \cup [c_n^+, c_n^-] \cup [c_n^-, b_n^-]$ 时有

$$\left|\frac{\Gamma'(1-s)}{\Gamma(1-s)}\right| \leqslant \pi + C_1 + \log|1-s| \leqslant \pi + C_1 + \log\sqrt{(2n+c)^2 + (n+1)^2} \leqslant \pi + C_1 + \log 3 + \log n.$$

- 如果 s 属于 $[b_n^+, c_n^+]$ 或者 $[c_n^-, b_n^-]$, 我们有 $|\mathrm{Im}(s)| \geqslant n$, 从而

$$\left|\frac{e^{i\pi(s-c)/2} + e^{-i\pi(s-c)/2}}{e^{i\pi(s-c)/2} - e^{-i\pi(s-c)/2}}\right| \leqslant \frac{e^{\pi n/2} + e^{-\pi n/2}}{e^{\pi n/2} - e^{-\pi n/2}} \leqslant \frac{1+e^{-\pi}}{1-e^{-\pi}}.$$

如果 $s \in [c_n^+, c_n^-]$, 且 $s = c + 1 - 2n + it$, 则

$$\left|\frac{e^{i\pi(s-c)/2} + e^{-i\pi(s-c)/2}}{e^{i\pi(s-c)/2} - e^{-i\pi(s-c)/2}}\right| = \left|\frac{e^{-\pi t/2} - e^{\pi t/2}}{e^{-\pi t/2} + e^{\pi t/2}}\right| \leqslant 1 \leqslant \frac{1+e^{-\pi}}{1-e^{-\pi}}.$$

[437] 由此得到当 $s \in [b_n^+, c_n^+] \cup [c_n^+, c_n^-] \cup [c_n^-, b_n^-]$ 时有不等式 $|\frac{L'(s)}{L(s)}| \leqslant \log B + c(2) + \pi + C_1 + \log 3 + \frac{\pi}{2}\frac{1+e^{-\pi}}{1-e^{-\pi}} + \log n$. 故有结论. □

3. 在临界带中的函数 L

引理 A.3.6. — *设 F 是一个在包含了带状集 $a \leqslant \mathrm{Re}(s) \leqslant b$ 的开集上的全纯函数, 并假设在直线 $\mathrm{Re}(s) = a$ 和 $\mathrm{Re}(s) = b$ 上 $|F(s)| \leqslant M$, 且存在 $c, C > 0$ 使得当 $a \leqslant \sigma \leqslant b$ 和 $|\tau| \geqslant 1$ 时有 $|F(\sigma + i\tau)| \leqslant Ce^{c|\tau|}$. 于是在整个这条带上有 $|F(s)| \leqslant M$.*

证明 如果 $\varepsilon > 0$, 则由于 $\mathrm{Re}(\varepsilon s^2) \sim -\varepsilon \mathrm{Im}(s)^2$ 趋向 $-\infty$ 的速度比 $c|\mathrm{Im}(s)|$ 要快很多, 故当 s 在此带中趋向 ∞ 时 $|F(s)e^{\varepsilon s^2}|$ 趋向 0. 最大值原理 (注记 V.3.12) 让我们得到: 如果 T 足够大, 则 $|F(s)e^{\varepsilon s^2}|$ 在以 $a \pm iT$ 和 $b \pm iT$ 为顶点的矩形上的最大值在竖直线段上达到, 因此 $|F(s)e^{\varepsilon s^2}|$ 在这条带中的最大值在直线 $\mathrm{Re}(s) = a$ 或者 $\mathrm{Re}(s) = b$ 上达到. 由此推出 $|F(s)e^{\varepsilon s^2}| \leqslant M \sup(e^{\varepsilon a^2}, e^{\varepsilon b^2})$, 其中任意 $\varepsilon > 0$, 而 s 在带 $a \leqslant \mathrm{Re}(s) \leqslant b$ 中. 令 ε 趋向 0 便证明了 $|F|$ 在此带上被 M 控制, 这即为要证明的. □

引理 A.3.7. — *如果 $a < 0$, 则函数 $(s-a+1)^{a-\frac{3}{2}}(s-1)L(s)$ 在半平面 $\mathrm{Re}(s) \geqslant a$ 上有界.*

证明 由于 $\frac{3}{2} - a \geqslant 1$, 且由于 L 在半平面 $\mathrm{Re}(s) \geqslant 1-a$ 上有界, 故函数 $F(s) = (s-a+1)^{a-\frac{3}{2}}(s-1)L(s)$ 在半平面 $\mathrm{Re}(s) \geqslant 1-a$ 上有界 (从而特别地在直线

$\mathrm{Re}(s) = 1 - a$ 上有界). 另外, 根据引理 A.3.4, 函数 F 在直线 $\mathrm{Re}(s) = a$ 上有界. 最后, 函数 F 在带 $a \leqslant \mathrm{Re}(s) \leqslant 1 - a$ 上全纯以及性质 (L3) 证明了 F 满足引理 A.3.6 的条件 (其中 $b = 1 - a$, 而 c 为任意 $> c(a, 1 - a)$ 的实数). 于是得到结果. □

引理 A.3.8. — 存在 $C_1 > 0$ 使得 $\sup_{s \in D(2+it,12)} \left|\frac{L(s)}{L(2+it)}\right| \leqslant C_1 |t|^{21/2}$, 其中 $t \in \mathbf{R}$, $|t| \geqslant 15$. 而 (回忆)$D(2 + it, 12)$ 为中心在 $2 + it$ 半径为 12 的圆盘.

证明　由引理 A.3.7 得到 (其中 $a = -10$) 存在常数 C_1' 使得当 $\mathrm{Re}(s) \geqslant -10$ 时有

$$|L(s)| \leqslant C_1' \frac{|s + 11|^{23/2}}{|s - 1|}.$$

现在, 如果 $s \in D(2 + it, 12)$, 则有 $|s + 11| \leqslant |t| + 25$ 和 $|s - 1| \geqslant |s| - 1 \geqslant |t| - 13$. 更由于根据性质 (L1) 有 $|L(2 + it)^{-1}| \leqslant c(2)$, 我们得到, 如果 $|t| > 13$, 则

$$\sup_{s \in D(2+it,12)} \left|\frac{L(s)}{L(2 + it)}\right| \leqslant c(2) C_1' \frac{(|t| + 25)^{23/2}}{|t| - 13}.$$

推出结果已无任何问题. □

4. 在临界带中的函数 $\frac{L'}{L}$

[438]

引理 A.3.9. — (博雷尔 – 卡拉泰奥多里 (Borel-Carathéodory)) 设 Ω 是 $\mathbf{C}$ 中的一个开集, $R > 0$, 使得 $D(0, R) \subset \Omega$, 而 f 在 Ω 上全纯, 满足 $f(0) = 0$. 如果 $A = \sup_{|s|=R} \mathrm{Re}(f(s))$, 则

$$\left|\frac{f^{(k)}(s)}{k!}\right| \leqslant \frac{4AR}{(R - |s|)^{k+1}},$$

其中任意 $k \in \mathbf{N}$, 而 $s \in D(0, R^-)$.

证明　在 $D(0, R)$ 上有 $f(s) = \sum_{n=1}^{+\infty} a_n s^n$. 将 a_n 写成 $|a_n| e^{i\theta_n}$, 则得到 $\mathrm{Re}(f(Re^{i\theta})) = \sum_{m=1}^{+\infty} |a_m| R^m \cos(m\theta + \theta_m)$ 以及

$$\begin{aligned}
&\int_0^{2\pi} (1 + \cos(n\theta + \theta_m)) \mathrm{Re}(f(Re^{i\theta})) d\theta \\
&= \sum_{m=1}^{+\infty} |a_m| R^m \int_0^{2\pi} (1 + \cos(n\theta + \theta_n)) \cos(m\theta + \theta_m) d\theta = \pi |a_n| R^n.
\end{aligned}$$

由于 $0 \leqslant 1 + \cos(n\theta + \theta_n) \leqslant 2$, 由此可得出不等式 $\pi |a_n| R^n \leqslant 4\pi A$, 从而 $|a_n| \leqslant 4AR^{-n}$. (特别地, $A \geqslant 0$.) 现在, 如果 $|t| < R$, 则有

$$\left|\frac{f^{(k)}(s)}{k!}\right| = \left|\sum_{n=0}^{+\infty} \binom{n+k}{k} a_{n+k} s^n\right| \leqslant 4A \sum_{n=0}^{+\infty} \binom{n+k}{k} \frac{|s|^n}{R^{n+k}} = \frac{4AR}{(R - |s|)^{k+1}}.$$

即为所求. □

引理 A.3.10. — 设 Ω 是 $\mathbf{C}$ 的一个开集及 $R>0$, 使得 $D(0,3R)\subset\Omega$, 而 f 是 Ω 上满足 $f(0)=1$ 的全纯函数. 设 $M=\sup_{s\in D(0,3R)}|f(s)|$, Y 是 f 在 $D(0,R)$ 中的零点的集合. 于是:

$$\sum_{\rho\in Y} v_\rho(f)\leqslant\frac{\log M}{\log 2}\text{ 以及对任意的 } s\in D(0,R^-)\text{ 有 }\left|\frac{f'(s)}{f(s)}-\sum_{\rho\in Y}\frac{v_\rho(f)}{s-\rho}\right|\leqslant\frac{4R\log M}{(R-|s|)^2}.$$

证明 令 $g(s)=f(s)\prod_{\rho\in Y}(1-\frac{s}{\rho})^{-v_\rho(f)}$. 按此构造, g 在 $D(0,R)$ 中不取零, 且 $g(0)=1$; 因此存在 (参看命题 VI.2.3) 一个开集 $\Omega'\subset\Omega$ 包含了 $D(0,R)$ 和一个 Ω' 上的全纯函数 h 满足 $h(0)=0$ 并使得在 Ω' 上有 $g=e^h$. 设 $N=\sum_{\rho\in Y}v_\rho(f)$. 由于 $|1-s/\rho|\geqslant 2$, 如果 $|s|=3R$, 则有 $|g(s)|\leqslant 2^{-N}M$. 根据最大值原理 (注记 V.3.12) 这蕴含了 $1=|g(1)|\leqslant 2^{-N}M$, 从而 $N\leqslant\frac{\log M}{\log 2}$. 最后, 如果 $|s|=3R$, 则我们有 $|g(s)|\leqslant M$, 从而根据最大值原理 $\sup_{|s|=R}\leqslant M$, 并且 $\sup_{|s|=R}\operatorname{Re}(h(s))\leqslant\log M$. 引理 A.3.9 让我们由此可推出, 如果 $|s|<R$, 则 $|h'(s)|\leqslant\frac{4R\log M}{(R-|s|)^2}$, 并由于 $h'(s)=\frac{f'(s)}{f(s)}-\sum_{\rho\in Y}\frac{v_\rho(f)}{s-\rho}$, 故得到结论. □

如果 $n\in\mathbf{N}$, 以 Z_n 记 L 在圆盘 $D(2+in,4)$ 中的零点集合.

推论 A.3.11. — 存在常数 C_2,C_3 当 $|n|$ 充分大时, 使得

(i) $\sum_{\rho\in Z_n}v_\rho(L)\leqslant C_2\log|n|$;

(ii) 如果 $s\in D(2+in,\sqrt{10})$, 则 $|\frac{L'(s)}{L(s)}|\leqslant C_3\log|n|+C_2\log|n|(\inf_{\rho\in Z_n}|s-\rho|)^{-1}$.

[439] 证明 将引理 A.3.10 应用于 $f(s)=\frac{L(s+(2+in))}{L(2+in)}$ 和 $R=4$; 在此引理的记号下, 根据引理 A.3.8, 可以取 $M=C_1|n|^{21/2}$. 由此得到, 如果 $|s-(2+in)|\leqslant\sqrt{10}$ 有

$$\sum_{\rho\in Z_n}v_\rho(L)\leqslant\frac{\frac{21}{2}\log n+\log C_1}{\log 2}\text{ 和 }|\frac{L'(s)}{L(s)}|\leqslant\frac{16(\frac{21}{2}\log n+\log C_1)}{4-\sqrt{10}}+\sum_{\rho\in Z_n}\frac{v_\rho(L)}{|s-\rho|}.$$

因此得到结果. □

推论 A.3.12. — 存在 $C_4>0$, 且当 $n\in\mathbf{N}$ 充分大时存在 $t_n^+\in[n,n+1]$ 和 $t_n^-\in[-n-1,-n]$ 使得

$$\sup_{s\in[2+it_n^+,-1+it_n^+]}|\frac{L'(s)}{L(s)}|\leqslant C_4(\log n)^2\quad\text{和}\quad\sup_{s\in[-1+it_n^-,2+it_n^-]}|\frac{L'(s)}{L(s)}|\leqslant C_4(\log n)^2.$$

证明 由于 $|Z_n|\leqslant C_2\log n$, 线段 $]\operatorname{Im}(\rho)-\frac{1}{2C_2\log n},\operatorname{Im}(\rho)+\frac{1}{2C_2\log n}[$ 对于 $\rho\in Z_n$ 没有完全覆盖 $[n,n+1]$: 它们的并是一个长 $\leqslant 1$ 的开集. 于是存在 t_n^+ 使得 $|\operatorname{Im}(\rho)-t_n^+|\geqslant\frac{1}{2C_2\log n}$, 其中任意 $\rho\in Z_n$. 因此对于任意的 $s\in[2+it_n^+,-1+it_n^+]$ 有 $\inf_{\rho\in Z_n}|s-\rho|\geqslant\inf_{\rho\in Z_n}|\operatorname{Im}(s-\rho)|\geqslant\frac{1}{2C_2\log n}$. 同样地, 存在 $t_n^-\in[-n-1,-n]$ 使得对于任意的 $s\in[-1+it_n^-,2+it_n^-]$ 有 $\inf_{\rho\in Z_{-n}}|s-\rho|\geqslant\frac{1}{2C_2\log n}$. 引理 A.3.11 的 (ii) 让我们得到了结论 (譬如, 其中 $C_4=2C_2^2+1$). □

5. 结论

转到定理 A.3.3 的证明. 为了证明级数 $\sum_{\rho\in Y(L)}\frac{v_\rho(L)}{\rho(\rho+1)}$ 的收敛性, 我们观察到 $Y(L)$ 中的虚部在 n 和 $n+1$ 间的元的集合 Z'_n 被包含在圆盘 $D(2+in,4)$ 之中, 因此是 Z_n 的一个子集. 由于当 n 充分大时 $\sum_{\rho\in Z_n} v_\rho(L)\leqslant C_2\log|n|$, 故而从 $\sum_{n=1}^{+\infty}\frac{\log n}{n^2}$ 的收敛性得到 $\sum_{\rho\in Y(L)}\frac{v_\rho(L)}{\rho(\rho+1)}$ 的绝对收敛性.

现在, 对于每个充分大的 n 选取实数 t_n^+ 和 t_n^-, 满足推论 A.3.12 的结果. 令 a_n^+, b_n^+, c_n^+ 代表点 $2+it_n^+, -1+it_n^+, c+1-2n+it_n^+$, 而 a_n^-, b_n^-, c_n^- 代表点 $2+it_n^-, -1+it_n^-, c+1-2n+it_n^-$ (图 1). 我们记

- V_n 为竖直线段 $[c_n^+, c_n^-]$,
- A_n^+ 和 A_n^- 为水平线段 $[b_n^+, c_n^+]$ 和 $[c_n^-, b_n^-]$,

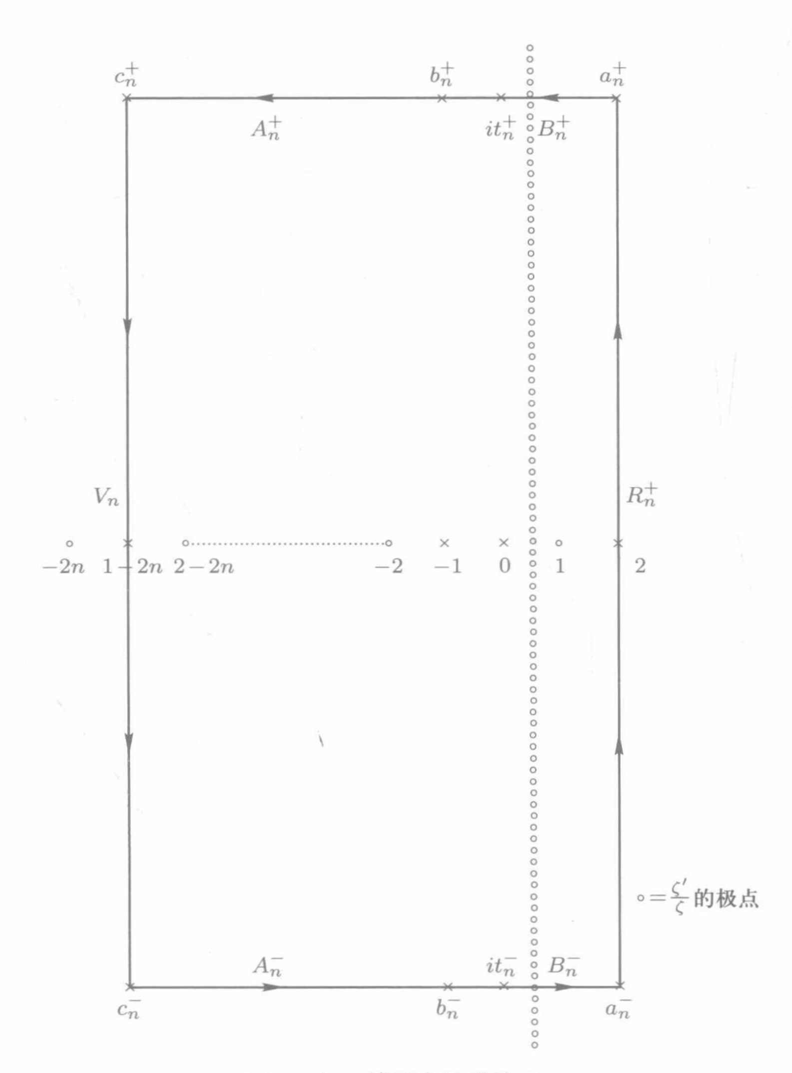


图 1. 在 ζ 情形中的道路 R_n

- B_n^+ 和 B_n^- 为水平线段 $[a_n^+, b_n^+]$ 和 $[b_n^-, a_n^-]$,
- R_n^- 为由线段 $B_n^+ \cdot A_n^+ \cdot V_n \cdot A_n^- \cdot B_n^-$ 组成的闭道,
- R_n^+ 为竖直线段 $[a_n^-, a_n^+]$.

于是 $R_n = R_n^+ \cdot R_n^-$ 是以 a_n^-, a_n^+, c_n^+ 和 c_n^- 为取正向的矩形的顶点. 以 Y_n 记位于矩形 R_n 内的 F_x 的极点的集合.

[440] 留数公式于是给出了

$$\int_{R_n} F_x(s)ds = \sum_{\rho \in Y_n} \operatorname{Res}(F_x, \rho).$$

现在, $\int_{R_n} F_x(s)ds = \int_{R_N^+} F_x(s)ds + \int_{B_n^+} F_x(s)ds + \int_{A_n^+ \cdot V_n \cdot A_n^-} F_x(s)ds + \int_{B_n^-} F_x(s)ds.$

- $\int_{R_n^+} F_x(s)ds$ 趋向 $\int_{2-i\infty}^{2+i\infty} -\frac{L'(s)}{L(s)} \frac{x^{s+1}}{s(s+1)} ds.$
- 根据推论 A.3.12, 在 B_n^+ 和 B_n^- 上, 当 $x \geqslant 1$ 时被 $C_4(\log n)^2 \frac{x^3}{|\operatorname{Im}(s)| \cdot |\operatorname{Im}(s+1)|} \leqslant \frac{x^3 C_4(\log n)^2}{n^2}$ 囿于上. 因此 $\int_{B_n^+} F_x(s)ds$ 和 $\int_{B_n^-} F_x(s)ds$ 的绝对值被 $3\frac{x^3 C_4(\log n)^2}{n^2}$ 囿于上, 从而当 n 趋向 $+\infty$ 时趋向 0.

[441]
- 在 $A_n^+ \cdot V_n \cdot A_n^-$ 上, 由于引理 A.3.5, 当 $x \geqslant 1$ 时, $F_x(s)$ 的绝对值被 $(C_0 + \log n)\frac{x^3}{|s(s+1)|} \leqslant (C_0 + \log n)\frac{x^3}{n^2}$ 囿于上, 并由于 $A_n^+ \cdot V_n \cdot A_n$ 的长为 $2(2n-2) + t_n^+ - t_n^- \leqslant 6n-2$, 由此推出当 n 趋向 $+\infty$ 时 $\int_{A_n^+ \cdot V_n \cdot A_n^-} F_x(s)ds$ 趋向 0.

令 n 趋向 $+\infty$ 并注意到 F_x 的极点集是 Y_n 的递增并, 从而 $\sum_{\rho \in Y_n} \operatorname{Res}(F_x, \rho)$ 趋向 $\sum_{\operatorname{Re}(\rho)<2} \operatorname{Res}(F_x, \rho)$, 那么由上面的分析便推出了定理.

习题 A.3.13. — 以 $\mathcal{N}(T)$ 记 ζ 函数的 s 在临界带中满足 $0 \leqslant \operatorname{Im}(s) \leqslant T$ 的零点数. 证明 $\mathcal{N}(T) = \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T)$. (考虑 $\frac{\xi'(s)}{\xi(s)} ds$ 的在以 $2+i, a_n^+, b_n^+$ 和 $-1+i$ 为顶点的矩形上的积分的虚部, 其中 $\xi(s) = \frac{\Gamma(s/2)}{\pi^{s/2}} \zeta(s)$, 并利用 ξ 的函数方程 (注记 VII.3.8 或习题 VII.6.6) 以及在复平面上的斯特林公式 (命题 VII.2.9) 和引理 A.3.10.)

A.4. 素数定理的证明

1. 在直线 $\operatorname{Re}(s) = 1$ 上不取零

引理 A.4.1. — 如果 $\alpha, \beta \in \mathbf{C}$, 且如果 $|z| < \inf(1, |\alpha|^{-1}, |\beta|^{-1}, |\alpha\beta|^{-1})$, 则

$$\frac{1 - \alpha\beta z^2}{(1-z)(1-\alpha z)(1-\beta z)(1-\alpha\beta z)} = \sum_{n=0}^{+\infty} (1 + \alpha + \cdots + \alpha^n)(1 + \beta + \cdots + \beta^n) z^n.$$

证明 在要证明的等式两端乘以 $(1-z)(1-\alpha z)(1-\beta z)(1-\alpha\beta z)$, 则得到形如 $\sum_{n=0}^{+\infty} P_n(\alpha, \beta) z^n$ 和 $\sum_{n=0}^{+\infty} Q_n(\alpha, \beta) z^n$, 其中 P_n 和 Q_n 是多项式 (两个变量的). 于是它化为证明对于所有 n 有 $P_n = Q_n$. 然而要证明 $P_n = Q_n$, 只要证明在一个开集上 $P_n = Q_n$ 即可, 而其余的则由解析延拓推出. 因此可以限制于 $1, \alpha, \beta$ 和 $\alpha\beta$ 互不相同

的情形. 在这种情形中, 有理分式 $F(z)=\frac{1-\alpha\beta z^2}{(1-z)(1-\alpha z)(1-\beta z)(1-\alpha\beta z)}$ 只有单极点, 将它分解为简单元时特别容易计算. 令

$$a_1=\lim_{z\to 1}(1-z)F(z)=\frac{1-\alpha\beta}{(1-\alpha)(1-\beta)(1-\alpha\beta)}=\frac{1}{(1-\alpha)(1-\beta)},$$
$$a_\alpha=\lim_{z\to\alpha^{-1}}(1-\alpha z)F(z)=\frac{1-\alpha^{-1}\beta}{(1-\alpha^{-1})(1-\alpha^{-1}\beta)(1-\beta)}=-\frac{\alpha}{(1-\alpha)(1-\beta)},$$
$$a_\beta=\lim_{z\to\beta^{-1}}(1-\beta z)F(z)=\frac{1-\alpha\beta^{-1}}{(1-\beta^{-1})(1-\alpha\beta^{-1})(1-\alpha)}=-\frac{\beta}{(1-\alpha)(1-\beta)},$$
$$a_{\alpha\beta}=\lim_{z\to\alpha^{-1}\beta^{-1}}(1-\alpha\beta z)F(z)=\frac{1-\alpha^{-1}\beta^{-1}}{(1-\alpha^{-1}\beta^{-1})(1-\beta^{-1})(1-\alpha^{-1})}=\frac{\alpha\beta}{(1-\alpha)(1-\beta)}.$$

因此, [442]

$$\begin{aligned}F(z)&=\frac{a_1}{1-z}+\frac{a_\alpha}{1-\alpha z}+\frac{a_\beta}{1-\beta z}+\frac{a_{\alpha\beta}}{1-\alpha\beta z}\\&=\frac{1}{(1-\alpha)(1-\beta)}\left(\frac{1}{1-z}-\frac{\alpha}{1-\alpha z}-\frac{\beta}{1-\beta z}+\frac{\alpha\beta}{1-\alpha\beta z}\right)\\&=\frac{1}{(1-\alpha)(1-\beta)}\sum_{n=0}^{+\infty}(1-\alpha^{n+1}-\beta^{n+1}+(\alpha\beta)^{n+1})z^n\\&=\sum_{n=0}^{+\infty}\frac{(1-\alpha^{n+1})(1-\beta^{n+1})}{(1-\alpha)(1-\beta)}z^n=\sum_{n=0}^{+\infty}(1+\alpha+\cdots+\alpha^n)(1+\beta+\cdots+\beta^n)z^n.\end{aligned}$$

□

命题 A.4.2. — 如果 $t\in\mathbf{R}$, 则 $F(s)=\zeta(2s)^{-1}\zeta(s)^2\zeta(s+it)\zeta(s-it)$ 是一个具有正系数的狄利克雷级数.

证明 利用 ζ 的欧拉因子的分解得到

$$F(s)=\prod_{p\in\mathscr{P}}\frac{(1-p^{-2s})}{(1-p^{-s})^2(1-p^{-s-it})(1-p^{-s+it})}.$$

于是可以利用引理 A.4.1, 其中 $z=p^{-s},\alpha=p^{it},\beta=p^{-it}$, 便得到了公式

$$F(s)=\prod_{p\in\mathscr{P}}\left(\sum_{k=1}^{+\infty}|1+p^{it}+\cdots+p^{ikt}|^2p^{-ks}\right),$$

从而得到结论. □

定理 A.4.3. — ζ 函数在直线 $\mathrm{Re}(s)=1$ 上不取零值.

证明 用归谬法, 假设存在 $t\in\mathbf{R}$, 满足 $\zeta(1+it)=0$. 因而有 $\zeta(1-it)=\overline{\zeta(1+it)}=0$, 函数 $\zeta(s+it)\zeta(s-it)$ 在 $s=1$ 有一个二阶零点, 这让 $F(s)=\zeta(2s)^{-1}\zeta(s)^2\zeta(s+it)\zeta(s-it)$ 在 $s=1$ 全纯: 这个二重点抵消了 $\zeta(s)^2$ 的极点. 同样,$\zeta(s)$ 在 $1+it$ 和

$1-it$ 的零点抵消了 $\zeta(s+it)$ 在 $1-it$ 和 $\zeta(s-it)$ 在 $1+it$ 的极点. 由此得到 $F(s)$ 在半平面 $\mathrm{Re}(s)>\frac{1}{2}$ 中全纯. 另外, 由于 $\zeta(2s)^{-1}$ 在 $s=\frac{1}{2}$ 的邻域中全纯, 并由于 F 的系数为正, 故由兰道定理 (定理 VII.1.1) 知, F 的绝对收敛横坐标 $<\frac{1}{2}$. 因为, 一方面由于在 $\frac{1}{2}$ 处 $\zeta(2s)^{-1}=0$, 故 $F(\frac{1}{2})=0$, 另一方面由于正项级数的和不取零, 故引出了矛盾. 证完. □

习题 A.4.4. — 设 χ 是 D 导子的狄利克雷特征标.

(i) 证明 $\zeta_D(2s)^{-1}\zeta_D(s)^2L(\chi,s+it)L(\overline{\chi},s-it)$ 是一个具有正系数的狄利克雷级数 (ζ_D 代表 ζ 去掉那些整除 D 的 p 的欧拉因子的函数, 即 $\zeta_D(s)=\prod_{p\in\mathscr{P},p\nmid D}\frac{1}{1-p^{-s}}$).

(ii) 由此推出 $L(\chi,s)$ 在直线 $\mathrm{Re}(s)=1$ 上不取零.

[443] 2. 结论

根据引理 A.2.1, 要证明素数定理只要证明 $\psi_1(x)\sim\frac{x^2}{2}$ 即可. 现在, 由于 ζ 满足性质 (L1)—(L3) (参看引理 A.3.11), 推论 A.2.6 和定理 A.3.3 给予我们一个显式的表达式

$$\psi_1(x)=\frac{x^2}{2}-\frac{\zeta'(0)}{\zeta(0)}x+\frac{\zeta'(-1)}{\zeta(-1)}-\sum_{\rho\in Y(\zeta)}\frac{v_\rho(\zeta)x^{\rho+1}}{\rho(\rho+1)}-\sum_{r=1}^{+\infty}\frac{x^{1-2r}}{2r(2r-1)}.$$

由此得知, "$\psi_1(x)\sim\frac{x^2}{2}$" 等价于 "$\lim_{x\to+\infty}\sum_{\rho\in Y(\zeta)}\frac{x^{\rho-1}}{\rho(\rho+1)}=0$". 由于 ζ 在直线 $\mathrm{Re}(s)=1$ 上不取零, 故有 $\mathrm{Re}(\rho-1)<0$, 从而 $\lim_{x\to+\infty}\frac{x^{\rho-1}}{\rho(\rho+1)}=0$, 其中 $\rho\in Y(\zeta)$. 由于进一步有 $|\frac{v_\rho(\zeta)x^{\rho-1}}{\rho(\rho+1)}|\leqslant|\frac{v_\rho(\zeta)}{\rho(\rho+1)}|$, 并因为 $|\frac{v_\rho(\zeta)}{\rho(\rho+1)}|$ 的和收敛, 故可以利用控制收敛定理得到取和与取极限交换. 从而得到结论.

习题 A.4.5. — 修改上面的推理以证明算术级数定理.

习题 A.4.6. — 建议从上面的显示表达式着手并利用级数 $\sum_{\rho\in Y(\zeta)}\frac{v_\rho(\zeta)}{\rho(\rho+1)}$ 的绝对收敛性证明素数定理蕴含了 ζ 在直线 $\mathrm{Re}(s)=1$ 上不取零的性质. 我们对 ζ 在直线 $\mathrm{Re}(s)=1$ 上的零点编号: 形如 $\rho=1+i\tau_n, n\in I, I\subset\mathbf{N}$, 并令 $a_n=\frac{v_{1+i\tau_n}(\zeta)}{(1+i\tau_n)(2+i\tau_n)}$.

(i) 证明, 如果 $\psi_1(x)\sim\frac{x^2}{2}$, 则 $\lim_{x\to+\infty}\sum_{n\in I}a_nx^{i\tau_n}=0$,

(ii) 由此推出 $\lim_{U\to+\infty}\frac{1}{U}\int_0^U|f(u)|^2du=0$, 其中 $f(u)=\sum_{n\in I}a_ne^{i\tau_nu}$,

(iii) 表达 $\lim_{U\to+\infty}\frac{1}{U}\int_0^U|f(u)|^2du$ 为 a_n 的函数,

(iv) 得到结论.

A.5. 补充

1. 黎曼假设及其推论

假定黎曼假设为真, 则在上面证明中出现的 ρ 的实部都等于 $\frac{1}{2}$, 于是这便让 $|\frac{v_\rho(\zeta)x^{\rho+1}}{\rho(\rho+1)}|$ 被 $x^{3/2}|\frac{v_\rho(\zeta)}{\rho(\rho+1)}|$ 囿于上, 而因为级数 $\sum_{\rho\in Y(\zeta)}\frac{v_\rho(\zeta)}{\rho(\rho+1)}$ 绝对收敛, 从而得到 $\psi_1(x)=\frac{1}{2}x^2+O(x^{3/2})$.

通过限制的不等式 $\psi_1(x)-\psi_1(x-1)\leqslant\psi(x)\leqslant\psi_1(x+1)-\psi_1(x)$ 和对于 $\psi_1(x)$ 的显式表达式则可以证明 $\psi(x)=x+O(x^{1/2}(\log x)^2)$.

最后, 利用下面的习题 A.5.2 我们可以证明以下结果, 而它则证明了黎曼假设对于素数分布的深刻意义.

命题 A.5.1. — 如果黎曼假设为真, 则 [444]

$$\pi(x)=\int_2^x\frac{1}{\log t}dt+O(x^{1/2}\log x).$$

习题 A.5.2. — 假定黎曼假设为真, 而我们将利用它的如下形式, 即 $\psi(x)=x+O(x^{1/2}(\log x)^2)$. 令 $A(x)=\sum_{p\leqslant x}\log p$ 及 $B(x)=A(x)-x$.

(i) 证明 $\psi(x)-A(x)=O(x^{1/2}\log x)$; 由此推出存在 $C>0$ 使得 $B(x)\leqslant Cx^{1/2}(\log x)^2$, 其中 $x\geqslant 2$.

(ii) 证明 $\pi(x)=\sum_{2\leqslant n\leqslant x}\frac{A(n)-A(n-1)}{\log n}$.

(iii) 由此推出

$$\pi(x)=\left(\sum_{2\leqslant n\leqslant n}\frac{1}{\log n}\right)+\frac{B([x])}{\log([x]+1)}+\left(\sum_{n=2}^{[x]}B(n)(\frac{1}{\log n}-\frac{1}{\log(n+1)})\right).$$

(iv) 得出结论.

注记 A.5.3. — 普森证明了, 存在 $c>0$ 使得 ζ 在 $\{s=\sigma+it,\sigma\geqslant 1-\frac{c}{\log(1+|t|)}\}$ 上不取零. 移动在此区域边界上的积分路径可以使素数定理中的误差项更精确些: 存在 $a>0$, 使得 $\pi(x)=\int_2^x\frac{1}{\log t}dt+O(x\exp(-a\sqrt{\log x}))$.

2. 黎曼假设和梅尔滕斯 (Mertens) 函数 M

回忆: 默比乌斯函数 μ 的定义是, 如果 $\mathrm{Re}(s)>0$, 则

$$\sum_{n=1}^{+\infty}\frac{\mu(n)}{n^s}=\zeta(s)^{-1}=\prod_{p\in\mathscr{P}}(1-p^{-s}).$$

因此当 n 被一个素数的平方整除时 $\mu(n)=0$, 而当 $n=p_1\cdots p_r$, 其中这些 p_i 互不相同时 $\mu(n)=(-1)^r$. 梅尔滕斯函数 M 定义为 $M(x)=\sum_{n\leqslant x}\mu(n)$, 而梅尔滕斯猜测,

如果 $x>1$, 则有 $|M(x)|\leqslant\sqrt{x}$. 这个猜想, 如果能确定为真, 则蕴含了黎曼假设. 事实上, 阿贝尔求和公式给出了

$$\zeta(s)^{-1}=\sum_{n=1}^{+\infty}M(n)(n^{-s}-(n+1)^{-s}),$$

那么, 梅尔滕斯猜想 $|M(n)|\leqslant\sqrt{n}$ 便意味着这个级数对于 $\mathrm{Re}(s)>\frac{1}{2}$ 绝对收敛, 从而 ζ 在 $\mathrm{Re}(s)>\frac{1}{2}$ 上不取零.

还不知道有任何对于梅尔滕斯猜想的显式反例, 但由于所谓的对数迭代律 (辛钦 (Khinchine),1924), 按照它, 如果 $a_n\in\{\pm1\}$, 且 $A_n=\sum_{k=1}^{n}a_n$, 则几乎成立

$$\limsup\frac{A_n}{\sqrt{2n\log\log n}}=1\quad \text{和}\quad \liminf\frac{A_n}{\sqrt{2n\log\log n}}=-1.$$

事实上, A.Odlyzko 和 H.te Riele 在 1985 年证明了梅尔滕斯猜想不成立, 知道存在小 [445] 于 $3\cdot21\cdot10^{64}$ 的一些反例. 一方面, 对数迭代律或者在第 VII 章的脚注提到的豪斯多夫的结果却使得黎曼假设更加合理. 另一方面, Odlyzko 和 te Riele 的结果也从数值上对黎曼假设做了一点相对的肯定 (它验证了 ζ 函数在临界带中的头 10^{13} 个零点确实是在直线 $\mathrm{Re}(s)=\frac{1}{2}$ 上).

3. 林德勒夫 (Lindelöf) 假设

它是一个被黎曼假设蕴含的猜想, 它原本就更弱. 它等价于以下的陈述中的一个 (要证明这些陈述的等价性需要做相当多的工作).

- 在 $+\infty$ 的邻域中, 对任意的 $\varepsilon>0$ 有 $|\zeta(\frac{1}{2}+it)|=O(t^{\varepsilon})$.
- 如果 $\sigma>\frac{1}{2}$, 且 $\mathcal{N}(\sigma,T)$ 代表 ζ 函数在满足 $\mathrm{Re}(s)\geqslant\sigma$ 和 $0\leqslant\mathrm{Im}(s)\leqslant T$ 的零点的个数, 则当 $T\to+\infty$ 时有 $\mathcal{N}(\sigma,T+1)-\mathcal{N}(\sigma,T)=o(\log T)$.
- 在 $+\infty$ 的邻域中, 对任意的 $\varepsilon>0$ 有 $\sum_{n\leqslant t}n^{-(\frac{1}{2}+2i\pi t)}=O(t^{\varepsilon})$.

我们可以将习题 A.3.13 与上面的第二个陈述进行比较, 而这个陈述是黎曼假设的推论, 后者可叙述为对热议的 $\sigma>\frac{1}{2}$ 和 $T\geqslant0$ 有 $\mathcal{N}(\sigma,T)=0$. 第三个陈述仅涉及有限和从而具有一个清楚简明的状态.

与黎曼假设相反, 林德勒夫假设隔一段时间就有一些进展. 例如, G. Kolesnik 在 1982 年证明了

$$\zeta(1/2+it)=O(t^{1/6-1/216+\varepsilon}),$$

其中任意 $\varepsilon>0$.

F. Bombieri 和 H. Iwaniec 在 1986 年证明了

$$\zeta(1/2+it)=O(t^{1/6-1/28+\varepsilon}),$$

其中任意 $\varepsilon>0$.

附录 B. $\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$ 的体积

本附录致力于计算 $\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$ 的体积, 这是西格尔 (Siegel, 1945) 的结果 (这个概念的准确意义将在以后见到). 这个计算是按照韦伊 (1946) 的想法并灵巧地利用了泊松公式, 通过对 n 的归纳进行的. 这个结果 (定理 B.1.4) 与群 $\mathbf{SL}_n(\mathbf{F}_p)$ 的基数公式 (命题 B.1.1) 紧密相关: 在适当的解释下, 这个公式是说, 群 $\mathbf{SL}_n(\mathbf{Z}_p)$ 的体积为 $\prod_{k=2}^n(1-\frac{1}{p^k})$, 并且 $\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$ 的体积的公式产生了一个乘积公式:[1]

$$\mathrm{Vol}(\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z}))\cdot\prod_{p\in\mathscr{P}}\mathrm{Vol}(\mathbf{SL}_n(\mathbf{Z}_p))=1.$$

它是一个非常一般性的公式的一个特殊情形 (其中有一些, 作为在引言中提及的布洛赫-加藤 (Bloch-Kato) 猜想, 大体上是推测性的), 它显示出实数世界和 p-adic 世界之间的至今仍十分神秘的深刻联系.

B.1. 算术对象的体积

1. 结果

命题 B.1.1. — 如果 K 是基数为 q 的有限域, 且 $n\geqslant 2$, 则

$$|\mathbf{SL}_n(K)|=q^{n-1}\prod_{k=2}^n(q^n-q^{n-k})=q^{n^2-1}\prod_{k=2}^n(1-\frac{1}{q^k}).$$

证明　从 $\mathbf{GL}_n(K)$ 到 K^* 的映射 $g\mapsto\det g$ 是一个满的群态射, 其核为 $\mathbf{SL}_n(K)$. 由于 $|K^*|=q-1$, 因此得到 $|\mathbf{SL}_n(K)|=\frac{1}{q-1}|\mathbf{GL}_n(K)|$.

---

[1] 如果 $\mathbf{A}$ 代表 $\mathbf{Q}$ 的阿代尔环 (参看 §G.2 的 1 小节), 则这个公式可以重写为令人印象深刻的公式 $\mathrm{Vol}(\mathbf{SL}_n(\mathbf{A})/\mathbf{SL}(\mathbf{Q}))=1$.

另外, 如果 $g \in \mathbf{GL}_n(K)$, 则 g 的 n 个列向量构成 K^n 的一组基, 从而得到从 $\mathbf{GL}_n(K)$ 到 K^n 的基的集合的一个双射. 由于 K^n 的一组基由第一个非零向量 e_1 (有 [448] $q^n - 1$ 种选法), 不属于由 e_1 生成的直线的第二个向量 e_2 (有 $q^n - q$ 种选法), 而第三个 e_3 不属于由 e_1 和 e_2 生成的空间 (有 $q^n - q^2$ 种选法),$\cdots\cdots$ 组成, 总共有 $(q^n-1)\cdots(q^n-q^{n-1})$ 个 K^n 的基.

得到所要结果. □

设 $n \geqslant 2$. 如果 $A \in \mathbf{M}_n(\mathbf{R})$ 且 $1 \leqslant \alpha, \beta \leqslant n$, 定义 (参看小词典的 7.6.2 小节) 余子式 $M_{\alpha,\beta}(A)$ 为 $(-1)^{\alpha+\beta}$ 乘以从 A 中抽去第 α 行和 β 列后得到的矩阵的行列式. 按第 α 行展开 $\det A$ 便得到

$$\det A = \sum_{j=1}^{n} x_{\alpha,j} M_{\alpha,j}(A).$$

为了减少烦琐的记号, 我们以 G 记 $\mathbf{SL}_n(\mathbf{R})$, Γ 记其子群 $\mathbf{SL}_n(\mathbf{Z})$.

如果 $1 \leqslant \alpha, \beta \leqslant n$, 以 $I(\alpha,\beta)$ 记集合 $\{1,\ldots,n\}^2 - \{(\alpha,\beta)\}$, 而 $E_{\alpha,\beta} = \mathbf{R}^{I(\alpha,\beta)}$ 表示 $(x_{i,j})_{(i,j)\in I(\alpha,\beta)}$ 构成的 $m = n^2 - 1$ 维的向量空间. 以 $\pi_{\alpha,\beta} : \mathbf{M}_n(\mathbf{R}) \to E_{\alpha,\beta}$ 记将 $(a_{i,j})_{1\leqslant i,j\leqslant n}$ 映成 $(a_{i,j})_{(i,j)\neq(\alpha,\beta)}$ 的线性映射. 由于 $M_{\alpha,\beta}$ 不涉及 $x_{\alpha,\beta}$, 于是我们也可以将 $M_{\alpha,\beta}$ 看成是 $E_{\alpha,\beta}$ 上的一个函数, 并以 $\Omega_{\alpha,\beta}$ 代表由 $M_{\alpha,\beta} \neq 0$ 定义的 $E_{\alpha,\beta}$ 中的一个开集. 如果 $x \in \Omega_{\alpha,\beta}$, 则上面对于 $\det A$ 的公式证明了存在唯一的 $\iota_{\alpha,\beta}(x) \in G$ 满足 $\pi_{\alpha,\beta}(\iota_{\alpha,\beta}(x)) = x$.

称 $\phi : G \to \mathbf{R}^+$ 可测是说 $\phi \circ \iota_{n,n}$ 在 $\Omega_{n,n}$ 上可测, 并定义 $\int_G \phi(g)dg$ 为 $\int_G \phi(g)dg = \int_{\Omega_{n,n}} \phi \circ \iota_{n,n} \frac{dx}{|M_{n,n}|}$.

命题 B.1.2. — *如果 $\phi : G \to \overline{\mathbf{R}}_+$ 可测, 则对于所有的 $\gamma \in G$, 有 $\int_G \phi(g\gamma)dg = \int_G \phi(g)dg = \int_G \phi(\gamma g)dg$. 换言之, dg 是 G 上的一个右和左的哈尔 (即不变) 测度.*

注记 B.1.3. — (n,n) 所处的特殊地位似乎有些奇怪, 但证明 dg 在乘以一个置换矩阵是不变的实际计算 (参看 §B.2 的 2 小节) 表明对于任意的 (α,β) 有 $\int_G \phi(g)dg = \int_{\Omega_{\alpha,\beta}} \phi \circ \iota_{\alpha,\beta} \frac{dx}{|M_{\alpha,\beta}|}$, 因而这种情形实际上是对称的.

如果 $\phi : G \to \mathbf{R}_+$ 对 Γ 是右不变的 (即对于 $g \in G$ 和 $\gamma \in \Gamma$ 有 $\phi(g\gamma) = \phi(g)$), 则 $\int_D \phi dg$ 不依赖 G/Γ 的基本区域的选取 (参看引理 B.1.5). 以 $\int_{G/\Gamma} \phi dg$ 表示这个量.

定义 $G/\Gamma = \mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$ 的体积为 $\mathrm{Vol}(G/\Gamma) = \int_{G/\Gamma} dg$.

定理 B.1.4. — *如果 $n \geqslant 2$, 则 $\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$ 有限, 并且由公式*

$$\mathrm{Vol}(\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})) = \prod_{k=2}^{n} \zeta(k)$$

给出.

2. 商空间上的积分

[449]

下面的引理 B.1.5 是我们在 §IV.3 (参看引理 IV.3.16) 的 2 小节中所给的定义在 $\mathbf{R}^n/\Lambda$ 上积分的推广, 其中 Λ 是一个格. 因为 G 上的积分定义为在 $\Omega_{n,n}$ 上的积分, 而由于 $\Omega_{n,n}$ 满足了以下的一些条件故可以将它应用到 G 上. 至于引理 B.1.6 及其推论则是在 $\mathbf{N}\times X$ 上的富比尼定理的翻版.

设 G 是一个具有右哈尔测度 (记为 dg) 的群: 假设这些对象满足

- G 上的正可测函数空间 $\mathrm{Mes}(G,\overline{\mathbf{R}}_+)$ 在整系数的线性组合下, 在 $(f,g)\mapsto \inf(f,g)$ 和 $(f,g)\mapsto \sup(f,g)$ 下, 以及在取单极限下稳定.
- 有由 $\mathrm{Mes}(G,\overline{\mathbf{R}}_+)$ 到 $\overline{R}_+$ 的一个积分,

  — 它是线性的: $\int_G(\lambda_1\phi_1+\lambda_2\phi_2)dg=\lambda_1\int_G\phi_1dg+\lambda_2\int_G\phi_2dg$, 其中 $\phi_1,\phi_2\in\mathrm{Mes}(G,\overline{\mathbf{R}}_+),\lambda_1,\lambda_2\geqslant 0$,

  — 满足单调收敛定理: $\int_G\sum_{i\in I}\phi_idg=\sum_{i\in I}\int_G\phi_idg$, 其中 I 为可数集, 而 ϕ_i 属于 $\mathrm{Mes}(G,\overline{\mathbf{R}}_+)$,

  — 在平移下不变: $\int_G\phi(g\gamma)dg=\int_G\phi(g)dg$, 其中 $\phi\in\mathrm{Mes}(G,\overline{\mathbf{R}}_+),\gamma\in\Gamma$.
- 可和函数空间 $\mathscr{L}^1(G)$ (即那些 $\phi: G\to\mathbf{C}$ 使得 $\mathrm{Re}^+(i^k\phi)$ 属于 $\mathrm{Mes}(G,\overline{\mathbf{R}}_+)$ 并满足 $\int_G\mathrm{Re}^+(i^k\phi)<+\infty$, 其中 $k\in\{0,1,2,3\}$) 和一个从 $\mathscr{L}^1(G)$ 到 $\mathbf{C}$ 的积分 $\phi\mapsto\int_G\phi dg$, 它的定义是 $\int_G dg=\sum_{i=0}^3 i^{-k}\int_G\mathrm{Re}^+(i^k\phi)dg$, 而它仍是线性的, 在右平移下不变, 且满足控制收敛定理.
- 可测集, 零测度集, 几乎处处 (或 a.e.) 为零的函数等概念像通常那样定义: $X\subset G$ 可测是说它的特征函数可测, 它为零测度集是说它可测且 $\int_X dg=0$(定义为 $\int_G \mathbf{1}_X dg$), 而 ϕ a.e. 为零是说 $\{g,\phi(g)\neq 0\}$ 的测度为零.

设 Γ 是 G 的一个可数子群. G/Γ 的一个基本区域 D 是 G 的一个可测子集使得我们可以将 G 的每个元 g 唯一地写成 $g=g_0\gamma$ 形式, 其中 $g_0\in D$ 而 $\gamma\in\Gamma$. 也可以将其重写为: 对所有的 $g\in G$ 有 $\sum_{\gamma\in\Gamma}\mathbf{1}_{D\gamma}(g)=1$, 其中 $D\gamma=\{g_0\gamma,g_0\in D\}$. 更一般地, G 的一个可测集 D 是 G/Γ 的一个近乎基本区域是指对每个 g *a.e.* 有 $g\mapsto\sum_{\gamma\in\Gamma}\mathbf{1}_{D\gamma}(g)=1$.

称 G 上的一个函数 ϕ 是在 Γ 下右不变的是说对于所有 $g\in G$ 和 $\gamma\in\Gamma$ 有 $\phi(g\gamma)=\phi(g)$.

引理 B.1.5. — 如果 $\phi: G\to\overline{\mathbf{R}}_+$ 可测并在 Γ 下右不变, 如果 D 是 G/Γ 的一个近乎基本区域, 则 $\int_D\phi dg$ 只与 D 有关.

证明 设 D_1,D_2 是 G 的两个子集且为 G/Γ 的两个近乎基本域. 依次应用: [450]

– 恒等式 $1=\sum_{\gamma\in\Gamma}\mathbf{1}_{D_2\gamma}$ *a.e.*,

– 单调收敛定理以交换取和与积分,

– 变量变换 $h=g\gamma$ 和 ϕ 与 dg 在此变换下的不变性,

– 再用单调收敛定理,

– 恒等式 $\sum_{\gamma\in\Gamma}\mathbf{1}_{D_1\gamma^{-1}}=1$ *a.e.*,

我们得到

$$\begin{aligned}\int_{D_1}\phi=\int_G\mathbf{1}_{D_1}\phi=\int_G\left(\sum_{\gamma\in\Gamma}\mathbf{1}_{D_2\gamma}\right)\mathbf{1}_{D_1}\phi=\sum_{\gamma\in\Gamma}\int_G\mathbf{1}_{D_2\gamma}\mathbf{1}_{D_1}\phi\\=\sum_{\gamma\in\Gamma}\int_G\mathbf{1}_{D_2}\mathbf{1}_{D_1\gamma^{-1}}\phi=\int_G(\sum_{\gamma\in\Gamma}\mathbf{1}_{D_1\gamma^{-1}})\mathbf{1}_{D_2}\phi\\=\int_G\mathbf{1}_{D_2}\phi=\int_{D_2}\phi,\end{aligned}$$

因此得到结论. □

如果 $\phi:G\to\overline{\mathbf{R}}_+$ 可测, 而且在 Γ 下不变, 那么我们以 $\int_{G/\Gamma}\phi dg$ 记 $\int_D\phi dg$, 其中 D 是 G/Γ 的近乎基本区域. 如果 $\phi:G\to\mathbf{C}$ 在 Γ 下右不变, 那么称 ϕ 在 G/Γ 上可和是说, 函数 $\mathrm{Re}^+(i^k\phi),k\in\{0,1,2,3\}$ 可测, 并满足 $\int_{G/\Gamma}\mathrm{Re}^+(i^k\phi)<+\infty$; 令 $\int_{G/\Gamma}\phi dg=\sum_{i=0}^3 i^{-k}\int_{G/\Gamma}\mathrm{Re}^+(i^k\phi)dg$.

引理 B.1.6. — 设 $\Gamma_1\subset\Gamma_2$ 是 G 的两个可数子群, 而 $\phi:G\to\overline{\mathbf{R}}_+$ 为可测函数, 并在 Γ_1 下右不变.

(i) 如果 $g\in G$, 则 $\sum_{s\in S}\phi(gs)\in\overline{\mathbf{R}}_+$ 与 Γ_2/Γ_1 在 Γ_2 中的代表系 S 的选取无关.

(ii) 如此定义的函数 $\int_{\Gamma_2/\Gamma_1}\phi$ 在 Γ_2 下右不变.

(iii) $\int_{G/\Gamma_1}\phi dg=\int_{G/\Gamma_2}(\int_{\Gamma_2/\Gamma_1}\phi)dg$.

证明　如果 S_1 和 S_2 是 Γ_2/Γ_1 的两个代表系, 则存在 (唯一的) 一个双射 $\alpha:S_1\to S_2$ 使得 $\theta(s_1)=\alpha(s_1)^{-1}s_1\in\Gamma_1$. 由此有

$$\sum_{s_1\in S_1}\phi(gs_1)=\sum_{s_1\in S_1}\phi(g\alpha(s_1)\theta(s_1))=\sum_{s_1\in S_1}\phi(g\alpha(s_1))=\sum_{s_2\in\alpha(s_1)}\phi(gs_2)=\sum_{s_2\in S_2}\phi(gs_2),$$

于是 (i) 得证.

现在, 如果 $\gamma\in\Gamma_2$, 且 S_1 是 Γ_2/Γ_1 的一个代表系, 那么 $S_2=\{\gamma s_1,s_1\in S_1\}$ 也同样是个代表系 (事实上, 如果 $s_1,s_1'\in S_1$, 且若存在 $\gamma_1\in\Gamma_1$ 使得 $\gamma s_1'=\gamma s_1\gamma_1$, 则 $s_1'=s_1\gamma_1$, 从而 $s_1'=s_1$, 这证明了 $S_2\to\Gamma_2/\Gamma_1$ 为单射; 又若 $\gamma'\in\Gamma_2$, 则存在 $s_1\in S_1$ [451] 使得 $\gamma^{-1}\gamma'\in s_1\Gamma_1$, 从而 $\gamma'\in\gamma s_1\Gamma_1$, 这证明了 $S_2\to\Gamma_2/\Gamma_1$ 为满射). 由此得到

$$\left(\int_{\Gamma_2/\Gamma_1}\phi\right)(g\gamma)=\sum_{s_1\in S_1}\phi(g\gamma s_1)=\sum_{s_2\in S_2}\phi(gs_2)=\left(\int_{\Gamma_2/\Gamma_1}\phi\right)(g).$$

这证明了 (ii).

转到 (iii) 的证明. 设 D 是 G/Γ_2 的一个基本区域而 S 是 Γ_2/Γ_1 的一个代表系. 由定义, 右端等于 $\int_D\sum_{s\in S}\phi(gs)dg$, 而由于 dg 在 G 的元的右平移下不变, 故它也等

于 $\int_{\Delta} \phi dg$, 其中 Δ 是对于 $s \in S$ 的 Ds 的不交并 (因为 $S \subset \Gamma_2$). 要得到结果, 因此只要证明 Δ 是 G/Γ_1 的基本区域即可. 然而

$$\sum_{\gamma_1 \in \Gamma_1} \mathbf{1}_{\Delta}(g\gamma_1) = \sum_{\gamma_1 \in \Gamma_1} \sum_{s \in S} \mathbf{1}_D(gs\gamma_1),$$

并且由于 S 是 Γ_2/Γ_1 的一个代表系, 则集合 $\{s\gamma_1, s \in S, \gamma_1 \in \Gamma_1\}$ 等于 Γ_2/Γ_1. 因此有 $\sum_{\gamma_1 \in \Gamma_1} \sum_{s \in S} \mathbf{1}_D(gs\gamma_1) = \sum_{\gamma_2 \in \Gamma_2} \mathbf{1}_D(g\gamma_2)$, 而由于 D 是 G/Γ_2 的基本区域, 于是最后面的这个量对于每个 g 等于 1. 得证. □

推论 B.1.7. — 设 $\phi: G \to \mathbf{C}$ 是在 Γ_1 下的右不变函数, 且在 G/Γ_1 上可和.

(i) 级数 $\sum_{s \in S} \phi(gs)$ 几乎处处绝对收敛, 其和与 Γ_2/Γ_1 在 Γ_2 中的代表系 S 的选取无关.

(ii) 如此定义的函数 $\int_{\Gamma_2/\Gamma_1} \phi$ *a.e.* 在 Γ_2 下右不变且在 G/Γ_2 上可和.

(iii) $\int_{G/\Gamma_1} \phi dg = \int_{G/\Gamma_2} (\int_{\Gamma_2/\Gamma_1} \phi) dg$.

证明 引理 B.1.6 的 (iii) 证明了 $\int_{G/\Gamma_2} (\int_{\Gamma_2/\Gamma_1} |\phi|) dg < +\infty$, 从而几乎处处成立 $\int_{\Gamma_2/\Gamma_1} |\phi| < +\infty$, 这证明了级数 $\sum_{s \in S} \phi(gs)$ 几乎处处绝对收敛. 剩下的由再次进行引理 B.1.6 的证明中的计算, 并利用对于绝对收敛的级数可重新任意排序的事实 (证明 (i) 和 (ii)) 以及控制收敛定理 (证明 (iii)). □

3. 逐步解开群 $\mathbf{SL}_n(\mathbf{R})$

设 $n \geqslant 2$. 以

- G' 记 $\mathbf{SL}_{n-1}(\mathbf{R})$.
- Γ' 记 G' 的子群 $\mathbf{SL}_{n-1}(\mathbf{Z})$.
- c (分别地, c') 记 G/Γ(分别地, G'/Γ') 的体积; 如果 $n = 2$, 则 $c' = 1$.

我们想要证明的是 $c = \zeta(n)c'$. 推论 B.1.10 让 c' 出现在 G/Γ 上的一个积分中. 为了使 c 与 c' 相关联, 我们由已知 G' 的方式去解开 G. 说得更准确点, 我们将证明 G 几乎等于 $W \times V \times G'$, 其中 W 和 V 分别是自然地同构于 $\mathbf{R}^n$ 和 $\mathbf{R}^{n-1}$ 的向量空间, 为此, 我们要引进以下的对象. [452]

- 设 W 是 n 行的列向量的空间. 将 $w \in W$ 映成它的坐标的 n-元组 $(w_1, \ldots, w_n)$ 的映射诱导了从 W 到 $\mathbf{R}^n$ 的自然同构; 以 W_* 表示由方程 $w_1 = 0$ 定义的超平面的补开集. 如果 $w \in W_*$ 的坐标为 $w_1, \ldots, w_n$, 以 $\alpha(w)$ 记对角线上除最后一个系数为 w_1^{-1} 外其余全为 1 的 $(n-1) \times (n-1)$ 对角矩阵, 并以 $\iota_W(w)$ 记分块矩阵 $\begin{pmatrix} w_1 & 0 \\ w' & \alpha(w) \end{pmatrix}$, 其中 w' 为坐标是 $w_2, \ldots, w_n$ 的列向量. 由于 $\det \alpha(w) = w_1^{-1}$, 故 $\det \iota_W(w) = 1$, 从而 $\iota_W(w) \in G$.
- 设 V 为具有 $n-1$ 列的行向量的空间. 经 $v \in V$ 映成它的坐标的 $(n-1)$-元

组 $(v_1,\dots,v_{n-1})$ 的映射诱导了 V 到 $\mathbf{R}^{n-1}$ 上的同构. 以 ι_V 表示将行向量 $v\in V$ 映到分块矩阵 $\begin{pmatrix}1 & v\\ 0 & 1_{n-1}\end{pmatrix}$. 稍加计算便可证明 ι_V 是从 V 到 G 的一个群态射 (即 $\iota_V(v_1+v_2)=\iota_V(v_1)+\iota_V(v_2)$).

- 以 $\iota_{G'}:G'\to G$ 为将 $g'\in G'$ 映成分块矩阵 $\begin{pmatrix}1 & 0\\ 0 & g'\end{pmatrix}$ 的群态射.
- 设 $g\in G$ 为其第一列系数是 $1,0,\dots,0$ 的元 g 的集合 $H\subset G$. 如果 $h=\begin{pmatrix}1 & v\\ 0 & g'\end{pmatrix}$, 定义 $\pi_V(h)\in V$ 和 $\pi_{G'}(h)\in G'$ 分别为 $\pi_V(h)=v$ 和 $\pi_{G'}(h)=g'$. 因此有 $h=\iota_{G'}(\pi_{G'}(h))\iota_V(\pi_V(h))$, 并且这是 h 的形如 $h=\iota_{G'}(g')\iota_V(v), g'\in G', v\in V$ 的唯一写法. 另外, $\pi_{G'}:H\to G'$ 是一个群态射, 且由于公式 $\begin{pmatrix}1 & v_1\\ 0 & g_1'\end{pmatrix}\begin{pmatrix}1 & v_2\\ 0 & g_2'\end{pmatrix}=\begin{pmatrix}1 & v_1g_2'+v_2\\ 0 & g_1'g_2'\end{pmatrix}$, 故有 $\pi_V(h_1h_2)=\pi_V(h_1)\pi_{G'}(h_2)+\pi_V(h_2)$.
- 设 $\pi_W:G\to W$ 是将 g 映成它的第一列的映射. G 在 π_W 下的像是 $W-\{0\}$, 并且在 W_* 上有 $\pi_W\circ\iota_W=\mathrm{id}$. 另外, $\pi_W(g_1)=\pi_W(g_2)$ 当且仅当存在 $h\in H$ 使得 $g_2=g_1h$: 事实上, 如果 $e_1,\dots,e_n$ 是 $W\cong\mathbf{R}^n$ 的标准基, 则 $\pi_W(g_1)=\pi_W(g_2)$ 等价于 $g_1(e_1)=g_2(e_1)$, 从而 $g_1^{-1}g_2(e_1)=e_1$, 于是等价于 $g_1^{-1}g_2\in H$.

如果 $(w,v,g')\in W_*\times V\times G'$, 令 $\varphi(w,v,g')$ 为分块矩阵 $\begin{pmatrix}w_1 & w_1v\\ w' & w'v+\alpha(w)g'\end{pmatrix}$. 由于 $\iota_V(v)\iota_{G'}(g')\in H$, 它表明 $\pi_W(\varphi(w,v,g'))=\pi_W(\iota_W(w))=w$. 反之, 如果 $\pi_W(g)\in W_*$, 则存在唯一的三元组 $(w,v,g')\in W_*\times V\times G'$ 使得 $g=\varphi(w,v,g')$. 更准确地, 即

$$w=\pi_W(g)\ \text{和}\ v=\pi_V(h),\ g'=\pi_{G'}(h),\ \text{其中}\ h=(\iota_W(\pi_W(g)))^{-1}g.$$

总之, φ 诱导了从 $W_*\times V\times G'$ (它几乎等于 $W\times V\times G'$) 到第一个系数非零的 $g\in G$ 的集合 $G_*=\pi_W^{-1}(W_*)$ (它几乎等于 G) 上的双射.

在经过变量变换的不太神秘的计算之后, 尽管写起来不太舒服 (如 3 小节的 [453] §B.2), 给出了以下的结果: 其中的 dw (分别地, dv) 是在 W (分别地, V) 上的勒贝格测度 $dw_1\cdots dw_n$ (分别地, $dv_1\cdots dv_{n-1}$), 而 dg' 是 $G'=\mathbf{SL}_{n-1}(\mathbf{R})$ 上在命题 B.1.2 中的测度 (将 n 换成 $n-1$).

引理 B.1.8. — 如果 $\phi:G\to\mathbf{R}_+$ 可测, 则

$$\int_G\phi dg=\int_{W_*\times\mathbf{R}^{n-1}\times G'}\phi\circ\varphi dwdvdg'.$$

4. 在 $\mathbf{R}^n$ 和在 $\mathbf{SL}_n(\mathbf{R})/\mathbf{SL}_n(\mathbf{Z})$ 上的积分

以 Λ 代表坐标在 $\mathbf{Z}$ 中的 V 的向量构成的子群; 它是 V 的一个格. 以 Θ 记 H 中坐标为整数的元的子集. 它是 H 的一个子群, 它也是 $h \in H$ 使得 $\pi_V(h) \in \Lambda$ 和 $\pi_{G'}(h) \in \Gamma'$ 的集合.

设 D' 和 D'' 分别为 G'/Γ' 和 V/Λ 的基本区域. 我们有 $\int_{D''} dv = 1$ (可取 $D'' = [0,1[^{n-1}$) 以及按 c' 的定义, 有 $\int_{D'} dg' = c'$.

引理 B.1.9. — 设 $\phi: \mathbf{R}^n \to \overline{\mathbf{R}}_+$ 是一个在 Θ 下右不变的可测函数, 则

$$\int_{\varphi(W_* \times D'' \times D')} \phi dg = \int_{G/\Gamma} (\int_{\Gamma/\Theta} \phi) dg.$$

证明 根据引理 B.1.6, 上式右端等于 $\int_{G/\Theta} \phi dg$, 因而只要证明 $\Delta_0 = \varphi(W_* \times D'' \times D')$ 几乎是 G/Θ 的基本区域即可. 我们将证明, 更为准确地, Δ_0 是 G_*/Θ 的一个基本区域.

因此它涉及证明 G_* 中的每个元可以以唯一的方式写成 $g = \iota_W(w_0)\iota_{G'}(g_0')\iota_V(v_0)\theta$ 形式, 其中 $w_0 \in W_*, g_0' \in D', v_0 \in D'', \theta \in \Theta$. 将 π_W 用于前面的等式我们看出它应该有 $w_0 = \pi_W(g)$, 从而可以将 g 写成 $\iota_W(w_0)h, h \in H$ 的形式. 由于 D' 是 G'/Γ' 的基本区域, 故存在唯一的 $g_0' \in D'$ 和 $\gamma \in \Gamma'$ 使得 $\pi_{G'}(h) = g_0'\gamma$. 因此有 $h = \iota_{G'}(g_0')\iota_V(v)\iota_{G'}(\gamma)$, 其中 $v \in V$ 被唯一地确定. 由于 D'' 是 V/Λ 的基本区域, 故存在唯一的 $v_0 \in V$ 和 $\nu \in \Lambda$, 使得 $v = v_0 + \nu$. 因此有 $g = \iota_W(w_0)\iota_{G'}(g_0')\iota_V(v_0)\theta$, 其中 $\theta = \iota_V(\nu)\iota_{G'}(\gamma) \in \Theta$. 这证明了存在 g 的一个我们所希望有的分解. 至于唯一性可重新进行上面的论证并利用在每一步的分解的唯一性即可. □

推论 B.1.10. — (i) 如果 $\phi: W \to \overline{\mathbf{R}}_+$ 可测, 则

$$c' \int_W \phi dw = \int_{G/\Gamma} (\int_{\Gamma/\Theta} \phi \circ \pi_W) dg.$$

(ii) 如果 $\phi: W \to \overline{\mathbf{R}}_+$ 可和, 则 $\int_{\Gamma/\Theta} \phi \circ \phi_W$ 在 G/Γ 上可和, 并且

$$c' \int_W \phi dw = \int_{G/\Gamma} (\int_{\Gamma/\Theta} \phi \circ \pi_W) dg.$$

证明 (ii) 由 (i) 形式地得到. 由于 $\phi \circ \pi_W$ 在 H 下从而在 Θ 下右不变, 故根据引理 B.1.9 右端的项等于 $\int_{\varphi(W_* \times D' \times D'')} \phi \circ \pi_W dg$. 引理 B.1.8 让我们可以重写最后的这个量为 $\int_{W_* \times D' \times D''} \phi \circ \pi_W \circ \varphi dw dv dx'$. 由于 $\pi_W \circ \varphi(w, v, x') = w$, 故可将这个三重积分写为 $\int_W \phi dw, \int_{D''} dv = 1$ 和 $\int_{D'} dx' = c'$ 的乘积, 推论得证. □ [454]

5. $\zeta(n)$ 的出现及最终的计算

如果 $g \in G$, g 的列构成了 W 在 $\mathbf{R}$ 上的一组基; 它们生成的子群 Λ_g 是 W 的一个格. 另外, 由于 $\det g = 1$, 故格 Λ_g 的体积为 1.

反之, 如果 Λ 是 W 的一个体积为 1 的格, 并且如果 $v_1,\dots,v_n$ 是 Λ 在 $\mathbf{Z}$ 上的一组定向基 (即 $\det(v_1,\dots,v_n)>0$), 则其列为 $v_1,\dots,v_n$ 的矩阵 g 是 G 中使得 $\Lambda_g=\Lambda$ 的元; 由此得到 $g\mapsto\Lambda_g$ 诱导了 G 到 W 的体积为 1 的格的集合上的一个满射.

现在, $\Lambda_{g_1}=\Lambda_{g_2}$ 当且仅当可以将 g_2 (分别地, g_1) 的列写成 g_1 (分别地, g_2) 的列的整系数的线性组合. 转换成矩阵的语言, 这表明存在矩阵 $A,B\in\mathbf{M}_n(\mathbf{Z})$ 使得 $g_2=g_1A$ 和 $g_1=g_2B$. 于是 $B=A^{-1}$, 并且因为 g_1 和 g_2 的行列式为 1 故 $A\in\Gamma$. 于是由此讨论知, 映射 $g\mapsto\Lambda_g$ 诱导了从 G/Γ 到 $\mathbf{R}^n$ 的体积为 1 的格的集合间的一个双射 (换句话说, G/Γ 可以被看作为 $W\cong\mathbf{R}^n$ 的体积为 1 的格的集合).

如果 Λ 是 W 的一个格, 称 Λ 的一个元 λ 是本原的是说它不能写成 $a\cdot\lambda'$ 的形式, 其中 $a\in\mathbf{N}$ 而 $\lambda'\in\Lambda$. 如果 $v_1,\dots,v_n$ 是 Λ 在 $\mathbf{Z}$ 上的一组基, 且若 $\lambda=a_1v_1+\dots+a_nv_n$, 则 λ 为本原的当且仅当这些 a_i 在它们的集合中互素, 在一般情形中, 如果 $a=\operatorname{lcm}(a_1,\dots,a_n)$, 则 $\lambda=a\lambda'$, 其中 λ' 为本原的. 由此得知, 如果以 Λ' 表示 Λ 中本原元的集合, 则 $\Lambda-\{0\}$ 是对于 $a\in\mathbf{N}-\{0\}$ 的 $a\Lambda'$ 的不交并.

现在, 如果 $\gamma\in\Gamma$, 则 $\pi_W(g\gamma)$ 是 g 列间的一个互素的整系数的线性组合; 因此它是格 Λ_g 的一个本原元. 另外, 由习题 10.16 (应用到所考虑的矩阵的转置) 得到, 如果 $\operatorname{lcm}(a_1,\dots,a_n)=1$, 则存在 $\gamma\in\Gamma$, 使它的第一行为 $(a_1,\dots,a_n)$. 由此得知, 映射 $\gamma\mapsto\pi_W(g\gamma)$ 诱导了从 Γ 到 Λ_g 的本原元的集合 Λ'_g 间的一个满射, 从而是从 Γ/Θ 到 Λ'_g 间的一个双射 (因为 $\Theta=\Gamma\cap H$ 和 $\pi_W(g_1)=\pi_W(g_2)$ 当且仅当 $g_1^{-1}g_2\in H$).

上面的讨论让我们可重写引理 B.1.10 为

$$c'\int_W\phi(w)dw=\int_{G/\Gamma}\left(\sum_{\lambda\in\Lambda'_g}\phi(\lambda)\right)dg.$$

[455] 当我们从 Λ'_g 转到 Λ_g 时因子 $\zeta(n)$ 便出现了. 为了实现这个过程, 我们将利用变量变换公式 (其中 $a\in\mathbf{R}_+^*$)

$$\int_W\phi(aw)dw=a^{-n}\int_W\phi(w)dw,$$

对 $a\in\mathbf{N}-\{0\}$ 取和则给出

$$\begin{aligned}\zeta(n)c'\int_W\phi(w)dw&=c'\sum_{a=1}^{+\infty}\int_W\phi(aw)dw\\&=\sum_{a=1}^{+\infty}\int_{G/\Gamma}\left(\sum_{\lambda\in\Lambda'_g}\phi(a\lambda)\right)dg=\int_{G/\Gamma}\left(\sum_{\lambda\in\Lambda_g-\{0\}}\phi(\lambda)\right)dg.\end{aligned}$$

根据闵可夫斯基引理 (定理 B.1.12), W 的一个对于原点对称的, 体积 $\geqslant 2^n$ 的凸集必包含 W 中任何体积为 1 的格的一个非零元. 如果将 ϕ 取作这样一个凸集的特征函数, 则对任意的 $g\in G$ 有 $\sum_{\lambda\in\Lambda_g-\{0\}}\phi(\lambda)\geqslant 1$; 由此推出不等式 $c=\int_{G/\Gamma}dg\leqslant 2^n\zeta(n)c'$; 特别表明 c 有限.

现在, 如果 ϕ 是 $W \cong \mathbf{R}^n$ 上的一个施瓦兹函数, 且若 $\hat{\phi}$ 代表 ϕ 的傅里叶变换, 则由泊松公式 (定理 IV.3.19, 其中令 $g^* = {}^{\mathrm{t}}g^{-1}$(参看引理 IV.3.13); 由于 Λ_g 的体积为 1, 故不出现) 有:

$$\sum_{\lambda\in\Lambda_g}\phi(\lambda) = \sum_{\lambda\in\Lambda_{g^*}}\hat{\phi}(\lambda).$$

对此利用 $\hat{\phi}(0) = \int_W \phi(w)dw$, 然后利用泊松公式, 最后以 $\hat{\phi}$ 代替 ϕ 应用第一个恒等式[2], 这给了我们

$$\begin{aligned}\zeta(n)c'\hat{\phi}(0) + c\phi(0) &= \int_{G/\Gamma}\left(\sum_{\lambda\in\Lambda_g}\phi(\lambda)\right)dg\\ &= \int_{G/\Gamma}\left(\sum_{\lambda\in\Lambda_{g^*}}\hat{\phi}(\lambda)\right)dg = \zeta(n)c'\hat{\hat{\phi}}(0) + c\hat{\phi}(0).\end{aligned}$$

这个公式对于任意的 ϕ 成立, 而傅里叶反演公式 $\hat{\hat{\phi}}(0) = \phi(0)$ 使我们得到了等式 [456]

$$c = \zeta(n)c',$$

这就是我们要证明的.

注记 B.1.11. — 由于 $\zeta(n)c' = c = \mathrm{Vol}(G/\Gamma)$, 转向上面的公式, 则已经证明了

$$\int_W \phi(w)dw = \frac{1}{\mathrm{Vol}(G/\Gamma)}\int_{G/\Gamma}\left(\sum_{\lambda\in\Lambda_g-\{0\}}\phi(\lambda)\right)dg.$$

换句话说, 函数 ϕ 在 $\mathbf{R}^n$ 上的积分是 ϕ 在格的非零点上的值的和在体积为 1 的格的集合上的平均值.

6. 闵可夫斯基引理

下面的这个结果是在数论中的一个十分令人难以置信的应用.

定理 B.1.12. — (闵可夫斯基引理) 设 $K \subset \mathbf{R}^m$ 是一个相对于原点对称的紧凸集. 如果 $\mathrm{Vol}(K) \geqslant 2^m$, 则 K 包含了 $\mathbf{Z}^m$ 中的一个非原点的点.

[2]这要求证明 $\int_{G/\Gamma}\phi(g^*)dg = \int_{G/\Gamma}(\phi(g))dg$. 为此, 以 $\varphi: G \to G$ 为微分同胚 $g \mapsto \varphi(g) = g^*$; 注意到有 $\varphi(hg) = \varphi(h)\varphi(g), g, h \in G$. 变量变换的公式给出了一个连续函数 $J: G \to \mathbf{R}_+^*$ 使得 $\int_G \phi dg = \int_G (\phi\circ\varphi)Jdg$. 如果 $h \in G$, dg 在左平移下的不变性给出了, 对于每个 $h \in G$ 与可和的 ϕ 有

$$\int_G \phi(\varphi(hg))J(hg)dg = \int_G \phi(\varphi(g))J(g)dg = \int_G \phi(g)dg = \int_G \phi(\varphi(h)g)dg = \int_G \phi(\varphi(h)\varphi(g))J(g)dg.$$

由于 $\varphi(hg) = \varphi(h)\varphi(g)$, 由此对于 $h, g \in G$ 得到 $J(hg) = J(g)$, 因此 J 为常量. 由于 $\varphi\circ\varphi = \mathrm{id}$, 由此得到 $J^2 = 1$, 从而对 G 上的所有可和函数 ϕ 有 $\int_G \phi(g^*)dg = \int_G(\phi(g))dg$. 为得出结论, 只需注意 $\varphi(\Gamma) = \Gamma$ 并且如果 $g \in G$ 和 $\gamma \in \Gamma$, 则有 $\varphi(g\gamma) = \varphi(g)\varphi(\gamma)$, 它表明 φ 将 G/Γ 的基本区域变换为 G/Γ 的一个基本区域.

证明 设若相反. 如果 $\boldsymbol{n} \in \mathbf{Z}^m$, 则令 $X_{\boldsymbol{n}} = \{\boldsymbol{n} + \frac{v}{2}, v \in K\}$. 于是, 当 $\boldsymbol{n}_1 \neq \boldsymbol{n}_2$ 时 $X_{\boldsymbol{n}_1}$ 与 $X_{\boldsymbol{n}_2}$ 不交: 事实上, 否则存在 $v_1, v_2 \in K$ 使得 $\boldsymbol{n}_1 + \frac{v_1}{2} = \boldsymbol{n}_2 + \frac{v_2}{2}$, 可将它重写为 $\frac{1}{2}(v_2 - v_1) = \boldsymbol{n}_1 - \boldsymbol{n}_2$, 以及应用 K 相对于原点的对称性得 $-v_1 \in K$, 又因为 K 为凸集, 故 $\boldsymbol{n}_1 - \boldsymbol{n}_2 \in K$. 由此得到, 对于 $\boldsymbol{n} = (n_1, \ldots, n_m), |n_i| \leqslant N$ 的 $X_{\boldsymbol{n}}$ 的并集 K_N 的体积等于 $(2N+1)^m \frac{\mathrm{Vol}(K)}{2^m}$: 因为每个 $X_{\boldsymbol{n}}$ 的体积为 $\frac{\mathrm{Vol}(K)}{2^m}$. 而一共有 $(2N+1)^m$ 个这样的 $X_{\boldsymbol{n}}$, 并且这些 $X_{\boldsymbol{n}}$ 两两不交. 另外, 由于 K 为紧的, 故存在 $C > 0$ 使得 K 包含在 $[-2C, 2C]^m$ 中. 这表明 $K_N \subset [-N-C, N+C]^m$, 从而 $\mathrm{Vol}(K_N) \leqslant (2N+2C)^m, N \in \mathbf{N}$.

- 如果 $\mathrm{Vol}(K) > 2^m$, 那么当 N 充分大时, 这与 $\mathrm{Vol}(K_N) = (2N+1)^m \frac{\mathrm{Vol}(K)}{2^m}$ 相矛盾, 从而得到结论.

- 如果 $\mathrm{Vol}(K) = 2^m$, 则只要将上面的结果应用到 K 的位似 λK, 其中 $\lambda > 1$ 充分小 (事实上, 由于 K 为紧的, 从 K 到 $\mathbf{Z}^m - \{(0, \ldots, 0)\}$ 的距离为严格正的, 因此当 $\lambda > 1$ 足够小时, λK 不包含 $\mathbf{Z}^m - \{(0, \ldots, 0)\}$ 中的任何元).

证完. □

B.2. $\mathbf{SL}_n(\mathbf{R})$ 的哈尔测度

我们将证明命题 B.1.2 中的测度 dg 是一个左和右的哈尔测度. dg 的左不变性经由转置可由右不变性得到. 因此只要证明它的右不变性即可, 并且, 由于对所有 [457] $\phi : G \to \mathbf{R}_+$ 满足 $\int_G \phi(g\gamma) dg = \int_G \phi(g) dg$ 的 $\gamma \in G$ 的集合是 G 的一个子群, 因此只要对生成 G 的 γ 的集合证明右不变性即可. 下面的引理 B.2.4 给出了一个合适的生成元系.

1. 平延和群 $\mathbf{SL}_n(K)$ 的结构

设 K 是个交换域, 一个平延 T 是 $\mathbf{M}_n(K)$ 中的一个元, 它的对角线上全为 1, 而在对角线外只有唯一的非零系数. 如果这个系数在第 i 行第 j 列上 $(i \neq j)$, 则 $T = 1 + \lambda N_{i,j}$, 其中 $N_{i,j}$ 是除了第 i 行第 j 列的系数为 1 外其余的系数全为 0 的矩阵. 由于 $N_{i,j}^2 = 0$, 故有 $T^{-1} = 1 - \lambda N_{i,j}$, 因此一个平延的逆仍是个平延. 由于一个平延是对角线上为 1 的上或下三角矩阵, 故一个平延的行列式等于 1; 因此它属于 $\mathbf{SL}_n(K)$. 下面的结果表明 $\mathbf{SL}_n(K)$ 的每个元都是有限个平延矩阵的乘积, 这对许多类问题是很有用的.

定理 B.2.1. — 如果 $n \geqslant 2$, 则平延矩阵生成了 $\mathbf{SL}_n(K)$.

证明 证明由对 n 的归纳进行. $n = 2$ 的情形来自下面的引理.

引理 B.2.2. — 如果 K 为域, 而 $A \in \mathbf{SL}_2(K)$, 则存在 $t, x, y, z \in K$ 使得有 $A = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$.

证明　我们从公式 $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+xy & x+z+xyz \\ y & 1+yz \end{pmatrix}$ 着手. 由此得知, 如果 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(K)$ 满足 $c \neq 0$, 则它是上面的那三个矩阵的乘积, 其中 $y = c, x = c^{-1}(a-1), z = c^{-1}(d-1)$, 于是取 $t = 0$ 即可. 如果 $c = 0$, 则以形如 $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -t & 1 \end{pmatrix}$ 乘 A 得到的新矩阵是像上面那样的三个矩阵的乘积. 得到结果. □

引理 B.2.3. — 设 $n \geqslant 3$.

(i) 形如

$$V(\lambda_1, \ldots, \lambda_{n-1}) = \begin{pmatrix} 1 & 0 & 0 & \cdots & \lambda_1 \\ 0 & 1 & 0 & \cdots & \lambda_2 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 1 & \cdots & \lambda_{n-1} \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

或

$$H(\lambda_1, \ldots, \lambda_{n-1}) \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_{n-1} & 1 \end{pmatrix}$$

的矩阵是平延矩阵的乘积.

(ii) 对角矩阵 $\mathrm{Diag}(1, \ldots, 1, \lambda, \lambda^{-1}), \lambda \in K^*$ 是平延矩阵的乘积.

证明　对于 (i) 的证明, 只需注意 [458]

$$V(\lambda_1, \ldots, \lambda_{n-1}) = \prod_{i=1}^{n-1} (1 + \lambda_i N_{i,n}) \text{ 和 } H(\lambda_1, \ldots, \lambda_{n-1}) \prod_{i=1}^{n-1} (1 + \lambda_i N_{n,i})$$

即可.

对于 (ii) 的证明, 按照引理 B.2.2 可将矩阵 $\begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix}$ 写成 $\mathbf{SL}_2(K)$ 中的平延矩阵的乘积, 并通过在对角线上添加 1 其余添加 0, 将所得到的那些矩阵做成 $\mathbf{SL}_n(K)$ 中的元即可. □

回到定理的证明. 假定结果对于 $n-1$ 已得证, 现在要对 n 证明. 为此, 只要证明从任意一个矩阵 $M \in \mathbf{SL}_n(K)$ 出发, 并右乘选好的平延矩阵 $T_1, \ldots, T_m$, 并使得得到的矩阵是平延矩阵 $T_1' \cdots T_r'$: 事实上因此得到 $M = T_1' \cdots T_r' T_m^{-1} \cdots T_1^{-1}$, 其中的这些 T_i^{-1} 仍是平延的, 它给出了想要的写法.

由于 M 可逆, 它的列 $w_1, \ldots, w_n$ 是 K^n 的一个生成元族, 从而存在 $\lambda_1, \ldots, \lambda_n \in K$ 使得 $\lambda_1 w_1 + \cdots + \lambda_n w_n = {}^{\mathrm{t}}(0, \ldots, 0, 1)$. 有两种情形:

- $\lambda_1 = \cdots = \lambda_{n-1} = 0$, 这时 M 作为分块矩阵具有 $\begin{pmatrix} P_1 & 0 \\ v_1 & \lambda \end{pmatrix}$ 形式, 其中 $P_1 \in \mathbf{GL}_{n-1}(K), \lambda \in K^*$ 而 $v_1 \in K^{n-1}$(0 表示系数全为 0 的 n 行的列向量). 右乘 M 以 $\mathrm{Diag}(1, \ldots, 1, \lambda, \lambda^{-1})$, 根据引理 B.2.3, 后者也是平延矩阵的乘积, 这给出了一个形如 $\begin{pmatrix} P_2 & 0 \\ v & 1 \end{pmatrix}$ 的分块矩阵 M_2, 其中 $P_2 \in \mathbf{SL}_{n-1}(K)$(因为 M_2 的行列式等于 1), 而 $v \in K^{n-1}$.

- 存在 $i \leqslant n-1$ 的 $\lambda_i \neq 0$. 右乘 M 以 $(1 + \frac{\lambda_n - 1}{\lambda_i} N_{n,i}) V(\lambda_1, \ldots, \lambda_{n-1})$, 后者按引理 B.2.3 是平延矩阵的乘积, 给出了最后一列为 $v = \lambda_1 w_1 + \cdots + \lambda_i (w_i + \frac{\lambda_n - 1}{\lambda_i} w_n) + \lambda_{n-1} w_{n-1} + w_n = {}^{\mathrm{t}}(0, \ldots, 0, 1)$ 的一个矩阵 M_2, 从而也有形如上面的分块矩阵 $\begin{pmatrix} P_2 & 0 \\ v & 1 \end{pmatrix}$.

现在, 如果以 v_i 记 P_2 的第 i 行, 那么这些 v_i 构成 K^{n-1} 的一组基, 并存在 (唯一的)$\lambda_1, \ldots, \lambda_{n-1} \in K$ 使得 $v + \lambda_1 v_1 + \cdots + \lambda_{n-1} v_{n-1} = 0$. 左乘 M_2 以 $H(\lambda_1, \ldots, \lambda_{n-1})$, 后者按引理 2.3 是平延矩阵的乘积, 给出了分块矩阵 $M_3 = \begin{pmatrix} P_3 & 0 \\ 0 & 1 \end{pmatrix}$, 其中 $P_3 = P_2 \in \mathbf{SL}_{n-1}(K)$.

剩下来只是应用归纳假设将 P_3 写为在 $\mathbf{SL}_{n-1}(K)$ 中的平延矩阵的乘积, 并以在对角线上添加 1 而其余添加 0 扩充此矩阵, 从而得到了 $\mathbf{SL}_n(K)$ 中的元. 如此便得到了 M_3 的一个平延乘积的写法, 证完. □

以 $e_1, \ldots, e_n$ 表示 K^n 的标准基. 令 W 为满足以下性质的 $\mathbf{R}^n$ 的自同态 w 的矩阵的集合: 存在 $\sigma \in S_n$ 和 $\varepsilon_1, \ldots, \varepsilon_n \in \{\pm 1\}$ 满足 $w(e_i) = \varepsilon_i e_{\sigma(i)}$. 于是 W 是一个群且 W 中元的行列式等于 ± 1. 以 W^+ 记 W 与 $\mathbf{SL}_n(K)$ 的交.

[459] W 的元使得坐标轴 Ke_i 交换. 对于 $i \in \{1, \ldots, n\}$, 这给出了从 W 到 S_n 的一个满态射, 其核是系数为 1 或 -1 的对角矩阵. 这个态射在 W^+ 上的限制也是满的: 如果 $\sigma \in S_n$ 的符号为 $\varepsilon \in \{\pm 1\}$, 则将 e_1 映到 $\varepsilon e_{\sigma(1)}$, e^i 映到 $e_{\sigma(i)}, i \neq 1$ 是 W^+ 中的一个元, 其在 S_n 中的像为 σ.

引理 B.2.4. — $\mathbf{SL}_n(K)$ 由 W^+ 和 $1 + \lambda N_{1,2}$, $\lambda \in K$ 生成.

证明 设 $i \neq j$ 为 $\{1, \ldots, n\}$ 中的两个元, 而 $\sigma \in S_n$ 使得 $\sigma(1) = i$, $\sigma(2) = j$. 设 $w \in W^+$ 在 S_n 中的像为 σ, 从而存在 $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$ 使得 $w(e_1) = \varepsilon_1 e_i$, $w(e_2) = \varepsilon_2 e_j$.

以 $u_{i,j}$ 记 K^n 的矩阵为 $N_{i,j}$ 的自同态; 因此有 $u_{i,j}(e_j)=e_i$, $u_{i,j}(e_k)=0, k\neq j$. 由此推出, 当 $k\neq j$ 时有 $wu_{1,2}w^{-1}(e_k)=0$: 因为 $w^{-1}(e_k)=\pm e_{\sigma^{-1}(k)}$, 且 $\sigma^{-1}(k)\neq 2$ 以及 $wu_{1,2}w^{-1}(e_j)=\varepsilon_1\varepsilon_2 e_i$. 由此得到 $wN_{1,2}w^{-1}=\varepsilon_1\varepsilon_2 N_{i,j}$ 和 $w(1+\lambda N_{1,2})w^{-1}=1+\varepsilon_1\varepsilon_2\lambda N_{i,j}$. 这便得到由 W^+ 和 $1+\lambda N_{1,2}, \lambda\in K$ 生成的 $\mathbf{SL}_n(K)$ 的子群包含了所有的平延矩阵从而生成了 $\mathbf{SL}_n(K)$. 证完. □

2. dg 在平移下的不变性

按照引理 B.2.4, 要证明 dg 的右不变性只需证明对所有的 $\phi: G\to\mathbf{R}_+, \gamma\in W^+$ 和 $\gamma=1+\lambda N_{12}$ 有 $\int_G\phi(g\gamma)dg=\int_G\phi(g)dg$ 即可.

• 如果 $\gamma\in W^+$, 可将它写成 $\mathrm{Diag}(\varepsilon_i)A_\sigma$ 的形式, 其中 ε_i 是 $\{\pm1\}$ 中的元, $\sigma\in S_n$, 而 A_σ 是矩阵 $(a_{i,j})_{1\leqslant i,j\leqslant n}$, 其中当 $i\neq\sigma(j)$ 时 $a_{i,j}=a_{j,i}=0$, 但 $a_{\sigma(i),i}=1$. 以 $\mathrm{Diag}(\varepsilon_i)$ 右乘一个矩阵等于第 i 列乘以 ε_i, 而右乘 A_σ 等于交换了列: BA_σ 的第 i 列是 B 的第 $\sigma(i)$ 列. 由此得到 $M_{n,n}(B\gamma)=\pm M_{n,\sigma(n)}(B)$.

设 $\Omega_n=\cap_{i=1}^n\Omega_{n,i}$. 按照下面的引理 B.2.5, $\Omega_{n,n}-\Omega_n$ 的测度为 0, 从而 $\int_G\phi(g)dg=\int_{\Omega_n}\phi\circ\iota_{n,n}dx$. 另外, $g\mapsto g\gamma$ 诱导了从 $\iota_{n,i}(\Omega_{n,i})$ 到 $\iota_{n,\sigma(i)}(\Omega_{n,\sigma(i)})$ 的一个双射, 因而 $\varphi(x)=\pi_{n,n}(\iota_{n,n}(x)\gamma)$ 是一个从 Ω_n 到 Ω_n 的微分同胚, 这个微分同胚的逆是 $\phi(x)=\pi_{n,n}(\iota_{n,n}(x)\gamma^{-1})$. 因此有

$$\int_G\phi(g\gamma)dg=\int_{\Omega_n}\tilde\phi(\varphi(x))\left|\frac{\wedge_{(i,j)\neq(n,n)}dx_{i,j}}{M_{n,n}(x)}\right|=\int_{\Omega_n}\tilde\phi(x)\left|\frac{\wedge_{(i,j)\neq(n,n)}(d\psi(x))_{i,j}}{M_{n,n}(\psi(x))}\right|.$$

然而

$$\frac{\wedge_{(i,j)\neq(n,n)}(d\psi(x))_{i,j}}{M_{n,n}(\psi(x))}=\pm\frac{\wedge_{(i,j)\neq(n,n)}dx_{i,\sigma(j)}}{M_{n,\sigma(n)}(x)}$$

和关系式 (由微分 $\det A=1$ 并利用 $\det A$ 对于作为对应余子式系数的 $x_{\alpha,\beta}$ 的线性性得到)

$$dx_{n,n}=\frac{-1}{M_{n,n}(x)}\sum_{(\alpha,\beta)\neq(n,n)}M_{\alpha,\beta}(x)dx_{\alpha,\beta}$$

证明了 [460]

$$\frac{\wedge_{(i,j)\neq(n,n)}dx_{i,\sigma(j)}}{M_{n,\sigma(n)}(x)}=\pm\frac{\wedge_{(i,j)\neq(n,n)}dx_{i,j}}{M_{n,n}(x)}$$

因此 $\int_G\phi(g\gamma)dg=\int_{\Omega_n}\tilde\phi(x)|\frac{\wedge_{(i,j)\neq(n,n)}dx_{i,j}}{M_{n,n}(x)}|=\int_G\phi(g)dg$.

• 如果 $\gamma=1+\lambda N_{1,2}$, 则 $B\gamma$ 的列除了第二列外均与 B 的列相同, 而第二列是由添加第一列的 λ 倍得到. 由此得知 $\varphi(x)=\pi_{n,n}(\iota_{n,n}(x)\gamma)$ 是从 $\Omega_{n,n}$ 到 $\Omega_{n.n}$ 的一个微分同胚, 其逆为 $\psi(x)=\pi_{n,n}(\iota_{n,n}(x)\gamma^{-1})$, 并且有 $M_{n,n}(\psi(x))=M_{n,n}(x)$ 和 $\wedge_{(i,j)\neq(n,n)}(d\psi(x))_{i,j}=\wedge_{(i,j)\neq(n,n)}dx_{i,j}$. 由此得到等式 $\int_G\phi(g\gamma)dg=\int_G\phi(g)dg$, 得到所证.

引理 B.2.5. — *如果 $P \in \mathbf{R}[X_1, \ldots, X_m]$ 非零, 且若 $Z = \{x \in \mathbf{R}^m, P(x) = 0\}$, 则 Z 为零测度集.*

证明 证明由对 m 的归纳进行. 因为当 $m = 1$ 时一个非零多项式的零点为有限个, 故结论显见. 假设 $m \geqslant 2$, 并将 $P(X)$ 写成 $\sum_{i=0}^{d} Q_i(X)X_n^i, Q_i \in \mathbf{R}[X_1, \ldots, X_{m-1}]$, 其中 $Q_d \neq 0$. 集合 $Y = \{y \in \mathbf{R}^{m-1}, Q_d(y) = 0\}$ 按归纳假定具有零测度, 而如果 $y \notin Y$, 则因为一个单变量非零多项式只有有限个零点, 函数 $x_n \mapsto \mathbf{1}_Z(y, x_n)$ 几乎处处为 0. 由此得到测度

$$\begin{aligned}\lambda(Z) &= \int_{Y\times\mathbf{R}} \mathbf{1}_Z + \int_{(\mathbf{R}^{m-1}-Y)\times\mathbf{R}} \mathbf{1}_Z \\ &= \int_{\mathbf{R}} \left(\int_Y \mathbf{1}_Z(y, x_n)dy\right) dx_n + \int_{\mathbf{R}^{m-1}-Y} \left(\int_{\mathbf{R}} \mathbf{1}_Z(y, x_n)\right) dy\end{aligned}$$

等于 0: 因为 $\int_Y \mathbf{1}_Z(y, x_n)dy \leqslant \lambda(Y) = 0$, 以及对每个 $y \in \mathbf{R}^{m-1} - Y$ 有 $\int_{\mathbf{R}} \mathbf{1}_Z(y, x_n)dx_n = 0$. 证完. □

3. 从 $\mathbf{SL}_{n-1}(\mathbf{R})$ 到 $\mathbf{SL}_n(\mathbf{R})$

在这一小节要证明引理 B.1.8 的变量变换公式. 以 $\Omega'_{n-1,n-1}$ 记 $\mathbf{R}^{(n-1)^2-1}$ 中的一个开集, 它由抽去一个 $(n-1) \times (n-1)$ 矩阵的第 $(n-1)$ 行第 $(n-1)$ 列得到的余子式 $M'_{n-1,n-1}$ 不等于零定义. 按 $\int_{G'}$ 的定义, 所要证明的这个恒等式的右端也等于 $\int_{U\times\mathbf{R}^{n-1}\times\Omega'_{n-1,n-1}} \phi \circ \varphi \circ \iota' \frac{dwdvdg'}{|M'_{n-1,n-1}|}$, 其中 $\iota'(w, v, x') = (w, v, g')$, 而 $g' = \iota'_{n-1,n-1}(x')$ 是在抽去在 $(n-1)$ 行和 $(n-1)$ 列上的坐标后, G' 中唯一的映成 x' 的元.

现在 $\tilde{\varphi} = \pi_{n,n} \circ \varphi \circ \iota'$ 诱导了从 $U \times \mathbf{R}^{n-1} \times \Omega'_{n-1,n-1}$ 到 $E_{n,n}$ 的开集 $X = \{x \in \Omega_{n.n}, x_{1,1} \neq 0\}$ 上的一个微分同胚, 其逆为 $x \mapsto (w(x), v(x), g'(x))$, 其中 $w(x) = \pi_W \circ \iota_{n,n}(x), v(x) = \pi_V(h(x))$, 以及 $g'(x) = \pi_{G'}(h(x))$, 而 $h(x) = \iota_W(w(x))^{-1}\iota_{n,n}(x)$. 然而由于 $\Omega_{n,n} - X$ 包含在一个超平面中, 故其测度为 0; 由此得到 $\int_G dg$ 也等于 $\int_X \phi \circ \iota_{n,n} \frac{dx}{|M_{n,n}|}$. 变量变换公式表明最后这个量也等于 $\int_{U\times\mathbf{R}^{n-1}\times\Omega'_{n-1,n-1}} \phi \circ$ [461] $\iota_{n,n} \circ \tilde{\varphi} \frac{J_{\tilde{\varphi}}dwdvdg'}{|M_{n,n}\circ\tilde{\varphi}|}$, 并因为 $\iota_{n,n} \circ \pi_{n,n}$ 在 $\pi_{n,n}^{-1}(\Omega_{n,n})$ 上等于恒同映射, 故 $\iota_{n,n} \circ \tilde{\varphi} = \iota_{n,n}\pi_{n,n} \circ \varphi \circ \iota' = \varphi \circ \iota'$, 因此下面的引理 B.2.6 让我们得到了结论.

引理 B.2.6. — (i) $M_{n,n}(\tilde{\varphi}(w, v, x')) = w_1 M'_{n-1,n-1}(x')$.

(ii) $|J_{\tilde{\varphi}}(w, v, x')| = |w_1|$.

证明 设 w'' 为坐标 $w_2, \ldots, w_{n-1}$ 的列向量, v'' 是坐标 $v_1, \ldots, v_{n-1}$ 的行向量, 而 g'' 是抽去 $\iota'_{n-1,n-1}(x')$ 的最后一行和最后一列得到的 $(n-2) \times (n-2)$ 矩阵. 于是 $M_{n,n}(\tilde{\varphi}(w, v, x'))$ 是分块矩阵 $\begin{pmatrix} w_1 & w_1 v'' \\ w'' & w''v'' + g'' \end{pmatrix}$ 的行列式. 将 v_i 乘以第一列移动

到第 $(i+1)$ 列不改变此行列式, 因此此行列式也是 $\begin{pmatrix} w_1 & 0 \\ w'' & g'' \end{pmatrix}$ 的行列式, 这就是说 $w_1 \det g''$. 由于 $\det g'' = M'_{n-1,n-1}(x')$, 按定义, 这证明了 (i).

为证明 (ii), 我们从公式

$$\bigwedge_{(i,j)\neq(n,n)} d(\tilde{\varphi}(w,v,x')_{i,j}) = \pm J_{\tilde{\varphi}}(w,v,x') \bigwedge_{1\leqslant i\leqslant n} dw_i \bigwedge_{1\leqslant j\leqslant n-1} dv_j \bigwedge_{(i,j)\neq(n-1,n-1)} dx'_{i,j}$$

着手. 由于 $\tilde{\varphi}(w,v,x') = \begin{pmatrix} w_1 & w_1 v \\ w' & w'v + \alpha(w)\iota'_{n-1,n-1}(x') \end{pmatrix}$, 故有

- 当 $1 \leqslant i \leqslant n$ 时 $d(\tilde{\varphi}(w,v,x')_{i,1}) = dw_i$,
- 当 $1 \leqslant j \leqslant n-1$ 时 $d(\tilde{\varphi}(w,v,x')_{1,j}) = w_1 dv_{j-1} +$ 含 dw_1 的项,
- 当 $2 \leqslant i \leqslant n-1$ 和 $2 \leqslant j \leqslant n$ 时 $d(\tilde{\varphi}(w,v,x')_{i,j}) = dx'_{i-1,j-1} +$ dw_i 和 dv_j 的线性组合,
- 当 $2 \leqslant j \leqslant n-1$ 时 $d(\tilde{\varphi}(w,v,x')_{n,j}) = w_1^{-1} dx'_{n-1,j-1} +$ dw_i 和 dv_j 的线性组合.

由此, 并利用 $\wedge$ 的交错多重线性性得到

$$\begin{aligned}
&\bigwedge_{(i,j)\neq(n,n)} d(\tilde{\varphi}(w,v,x')_{i,j}) \\
&= \pm \bigwedge_{1\leqslant i\leqslant n} dw_i \bigwedge_{1\leqslant j\leqslant n-1} (w_1 dv_j) \bigwedge_{1\leqslant i\leqslant n-2, 1\leqslant j\leqslant n-1} dx'_{i,j} \bigwedge_{1\leqslant j\leqslant n-2} (w_1^{-1} dx'_{n-1,j}) \\
&= \pm w_1 \bigwedge_{1\leqslant i\leqslant n} dw_i \bigwedge_{1\leqslant j\leqslant n-1} dv_j \bigwedge_{(i,j)\neq(n-1,n-1)} dx'_{i,j}.
\end{aligned}$$

证完. □

附录 C. 有限群与表示: 例子

这个附录想要解释研究有限群的表示的好处, 我们感兴趣的是三种群: 基数为 p 的幂的群, 在理论物理中有重要作用的对称群 S_n, 以及群 $\mathbf{GL}_2(\mathbf{F})$, 其中 $\mathbf{F}$ 是个有限域. 最后这个情形让我们去重温理论部分的第一章的主要结果.

C.1. p-群

1. p-群总论

设 p 是个素数. 一个 *p-群*是一个阶为 p 的幂的群.

命题 C.1.1. — (i) *如果 $G \neq \{1\}$ 是一个 p-群, 则 G 的中心非平凡.*

(ii) 如果 G 是个非交换 p-群, 则 G 包含一个正规的交换子群且此子群严格地包含了 G 的中心.

证明 (i) 让 G 以共轭作用于自身. 于是它的轨道是共轭类, 而中心 Z 是其共轭类化为单点的那些元 $c \in G$ 的集合. 已知 Z 包含了中性元, 而我们的问题便是要证明存在另一个可化为单点的共轭类. 现在, 如果 O 是一个共轭类, 且 $x \in O$, 于是 $O = G/Z_x$, 其中 Z_x 是 G 中与 x 交换的元的集合; 因此 $|O| = |G|/|Z_x|$, 这证明了 $|O|$ 是 p 的一个幂, 特别地, 除了 $|O| = 1$ 外, $|O|$ 被 p 整除. 由于 $|G|$ 被 p 整除, 并且是所有轨道的基数的和, 从而得知化为单点的轨道的集合的基数被 p 整除. 换句话说, $|Z|$ 被 p 整除, 而由于 $|Z| \geqslant 1$, 故有 $|Z| \geqslant p$; (i) 得证.

(ii) 现假设 G 非交换 (从而 $G \neq Z$), 并令 $H = G/Z$. 于是 H 是个 p-群, 其中心 Y 非平凡. 设 y 是 H 的中心中的一个不同于中性元的一个元, 并令 $\langle y \rangle$ 为由 y 生成的 Y 中的子群, 又设 A 为 $\langle y \rangle$ 在 G 中的逆像. 由于 $\langle y \rangle$ 在 H 中是正规的 (因为

是在中心中), 这表明 A 是 G 中的正规子群, 而且由于 A 严格包含了 Z, 故只需再证明 A 是交换的即可. 设 a 为 y 的阶, 并设 $\tilde{y} \in A$ 在 H 中的像为 y. 于是 $\langle y \rangle$ 的元为 $y^i, 0 \leqslant i \leqslant a-1$, 从而 A 的每个元都可以写成形如 $\tilde{y}^i z$ 的元, 其中 $0 \leqslant i \leqslant a-1$ 和 $z \in Z$. 如果 $x_1 = \tilde{y}^{i_1} z_1$, $x_2 = \tilde{y}^{i_2} z_2$, 那么考虑到 Z 中的元与所有的元交换, 则得到 [464]

$$x_1 x_2 = \tilde{y}^{i_1} z_1 \tilde{y}^{i_2} z_2 = \tilde{y}^{i_1} \tilde{y}^{i_2} z_2 z_1 = \tilde{y}^{i_1+i_2} z_2 z_1 = \tilde{y}^{i_2} z_2 \tilde{y}^{i_1} z_1 = x_2 x_1,$$

得到结论. □

2. p-群的表示

注记 C.1.2. — 设 G 是个有限群. 如果 A 是 G 的一个正规子群, 而 W 是 A 的一个表示, $g \in G$, 则我们可以构造一个 A 的表示 W^g: 令 $\rho_{W^g}(a) = \rho_W(g^{-1}ag)$; 由正规子群的定义知, 当 $a \in A, g \in G$ 时 $g^{-1}ag \in A$, 故这个定义是有意义的. 我们立刻得知, W^g 不可约当且仅当 W 不可约, 从而得到了 G 在 $\mathrm{Irr}(A)$ 上的一个作用 $(g, \chi) \mapsto \chi^g$. [如果 $\chi \in \mathrm{Irr}(A)$ 是一个不可约特征标, 则 $\chi^g(a) = \chi(g^{-1}ag)$.]

命题 C.1.3. — *设 G 为有限群, 而 A 是 G 的正规子群. 如果 V 是 G 的一个不可约表示且其在 A 上的限制 $\mathrm{Res}_G^A V$ 不是同型的, 则存在一个严格包含在 G 中的一个包含了 A 的子群 H, 以及一个 H 的不可约表示 W, 使得 $V = \mathrm{Ind}_H^G W$.*

证明　将 $\mathrm{Res}_G^A V$ 分解为它的同型分支的直和 $\oplus_{\chi \in X} V_\chi$, 其中 $X \subset \mathrm{Irr}(A)$. 由假设条件知, $|X| \geqslant 2$. 如果 $\chi \in X$, 且 $g \in G, a \in A$, 则有 $a \cdot (g \cdot V_\chi) = g \cdot (g^{-1}ag \cdot V_\chi)$, 这证明了 $g \cdot V_\chi$ 在 a 的作用下稳定, 且 $\rho_{g \cdot V_\chi}(a) = \rho_{V_\chi}(g^{-1}ag)$. 由此推出 g 将同型分支 V_χ 带到了同型分支 V_{χ^g} 上, 从而置换了 X 的元.

设 $\chi_0 \in X$, 且 W 是 $\mathrm{Res}_G^A V$ 的对应于 χ_0 的同型分支, 而 $H \subset G$ 是 χ_0 的稳定子. 于是 W 在 H 下稳定, 因此可以将其看成是 H 的一个表示. 现在, $\sum_{g \in G} g \cdot W = \oplus_{g \in G/H} V_{\chi_0^g}$ 在 G 下稳定, 从而, 因假设了 V 不可约, 故其等于 V. 由此得到 $X = G/H$, 于是 $H \neq G$, 以及 V 和 $\mathrm{Ind}_H^G W$ 具有相同的维数 $|X| \cdot \dim W$. 另外, $\mathrm{Hom}_H(W, V)$ 非零, 从而 $\mathrm{Hom}_G(\mathrm{Ind}_H^G W, V)$ 也非零 (习题 I.3.17). 由于 V 不可约且 $\mathrm{Ind}_H^G W$ 和 V 具有相同维数, 于是 $\mathrm{Hom}_G(\mathrm{Ind}_H^G W, V)$ 的每一个非零元诱导了 $\mathrm{Ind}_H^G W$ 到 V 的同构. 证完. □

命题 C.1.4. — *如果 G 是一个 p-群, 而 V 是 G 的一个不可约表示, 则存在 G 的一个子群 H 以及一个线性特征标 $\chi \in \hat{H}$ 使得 $V = \mathrm{Ind}_H^G \chi$.*

证明　由对 $|G|$ 的归纳进行证明. 如果 G 交换, 则每个不可约表示的维数均为 1, 没有什么需要证明的. 假设 G 非交换, 且设 V 是 G 的一个不可约表示.

[465] • 如果 ρ_V 的核 N 非平凡, 则 ρ_V 可通过 $G' = G/N$ 分解, 从而可将归纳假定应用到 G' 上: 存在 $H' \subset G'$ 和 $\chi \in \hat{H}'$ 使得作为 G' 的表示有 $V = \mathrm{Ind}_{H'}^{G'} \chi$. 如果 H 是 H' 在 G 中的逆像, 则可通过复合投射 $H \to H'$ 将 χ 看作是 $\hat{H}$ 中的元, 从而有

$V = \mathrm{Ind}_H^G\chi$, 从而得到在这种情形时的证明.

- 如果 ρ_V 的核平凡, 则考虑 G 的一个不包含在 G 的中心中的一个正规交换子群 A(参看 C.1.1 的 (ii)). 特别地, 存在 $a \in A$ 和 $g \in G$ 满足 $ag \neq ga$, 并由于 ρ_V 的核平凡, 故有 $\rho_V(a)\rho_V(g) \neq \rho_V(g)\rho_V(a)$. 这表明 $\rho_V(a)$ 不是一个位似变换, 从而作为交换的 A, $\mathrm{Res}_G^A V$ 不是同型的. 由此并利用命题 C.1.3 推出存在 G 的一个子群 H, 它包含 A 而不同于 G, 以及 H 的一个不可约表示 W, 使得 $V = \mathrm{Ind}_H^G W$. 对 H 应用归纳假设便给出了 H 的一个子群 H' 和 $\chi \in \hat{H}'$, 使得 $W = \mathrm{Ind}_{H'}^H\chi$. 注意到

$$V = \mathrm{Ind}_H^G(\mathrm{Ind}_{H'}^H\chi) = \mathrm{Ind}_{H'}^G\chi,$$

便得到了结论. □

习题 C.1.5. — 设 p 是个素数, 而 G 是个阶为 p^3 的非交换群. 证明 G 有 p^2 个一维的不可约表示和 $p-1$ 个 p 维的不可约表示.

C.2. 对称群 S_n 的表示

S_n 的表示理论涉及一些相当有趣的、远非平凡的组合数学. 我们也只限于描述结果而证明则让读者去参看那些更为专业的著作 (如在引言中引述的 Fulton 和 Harris 的书) (也可将此看作一系列的挑战 $\cdots\cdots$).

1. n 的分拆和 S_n 的表示

设 $n \geqslant 1$ 为整数. n 的一个分拆 $\boldsymbol{\ell} = (\ell_1, \ldots, \ell_r)$ 是 n 的一个分解 $n = \ell_1 + \cdots + \ell_r$, 其中 $\ell_1 \geqslant \ell_2 \geqslant \ldots \geqslant \ell_r \geqslant 1$. n 的分拆的个数按习惯记为 $p(n)$[1]. 例如, $1, 2, 3, 4, 5, 6$ 的分拆由下面给出:

[466]

1	4	5	6
	3+1	4+1	5+1
2	2+2	3+2	4+2
1+1	2+1+1	3+1+1	4+1+1
	1+1+1+1	2+2+1	3+3

[1]有许多工作是研究函数 $p(n)$ 的; 它们中大多数都是从公式

$$\sum_{n=1}^{+\infty} p(n)T^n = \prod_{\ell=1}^{+\infty} \frac{1}{1-T^\ell}$$

着手, 而对此公式的证明只需注意到 $\frac{1}{1-T^\ell} = \sum_{i=0}^{+\infty} T^{i\ell}$ 并直接展开右边的项即可, 这个公式还与戴德金 η 函数的逆有关, 其中的 η 定义为 $\eta(q) = q^{1/24}\prod_{\ell=1}^{+\infty}(1-q^\ell)$, 而这里的 $q = e^{2i\pi z}$, z 则在庞加莱半平面中变动. 利用 η 函数是一个权为 $\frac{1}{2}$ 的模形式的性质 (问题 H.11), 则可以, 譬如, 得到一个渐进等价 $p(n) \sim \frac{1}{4\sqrt{3}n}e^{\pi\sqrt{2n/3}}$. 这证明了 $p(n)$ 随 n 增大得足够快.

3	2+1+1+1	3+2+1
2+1	1+1+1+1+1	3+1+1+1
1+1+1		2+2+2
		2+2+1+1
		2+1+1+1+1
		1+1+1+1+1+1

因此有 $p(1)=1, p(2)=2, p(3)=3, p(4)=5, p(5)=7, p(6)=11$.

我们赋予 n 的分拆的集合以字典序, 其定义为 $\boldsymbol{\ell}=(\ell_1,\ldots,\ell_r)>\boldsymbol{k}=(k_1,\ldots,k_s)$ 当且仅当如果 i 是使得 $\ell_i\neq k_i$ 的最小指标, 则 $\ell_i>k_i$. 上面给出的 $1,2,3,4,5,6$ 的分拆正是按字典序以递降排列的. (这是能记住的最好方法.)

在 n 的分拆与 S_n 的共轭类之间有一个自然的双射 $\boldsymbol{\ell}\mapsto C_{\boldsymbol{\ell}}$: 如果 $\boldsymbol{\ell}=(\ell_1,\ldots,\ell_r)$, 则 $C_{\boldsymbol{\ell}}$ 是 S_n 中的分解为一些循环 $(\ell_1,\ldots,\ell_r)$ 的元 σ (回忆一下: 这表明 σ 是 r 个循环 $\tau_1,\ldots,\tau_r$ 的乘积, 而它们的长分别为 $\ell_1,\ldots,\ell_r$, 并且它们的支集是互不相交的).

也有一个非常好的方式给出在 n 的分拆和 S_n 的不可约表示间的自然双射. 如果 $\boldsymbol{\lambda}=(\lambda_1,\ldots,\lambda_s)$ 是 n 的一个分拆, 令 $S_{\boldsymbol{\lambda}}\cong S_{\lambda_1}\times\cdots\times S_{\lambda_s}$, 这是由 S_n 中让 $\{1,\ldots,n\}$ 的子集

$$\{1,\ldots,\lambda_1\},\{\lambda_1+1,\ldots,\lambda_1+\lambda_2\},\ldots,\{\lambda_1+\cdots+\lambda_{s-1}+1,\ldots,\lambda_1+\cdots+\lambda_s\}$$

中的每一个都稳定的置换构成, 又令 $U_{\boldsymbol{\lambda}}=\mathrm{Ind}_{S_{\boldsymbol{\lambda}}}^{S_n}\mathbf{1}$. 例如:

- 如果 $\boldsymbol{\lambda}=(n)$, 则 $U_{\boldsymbol{\lambda}}$ 是平凡表示.
- 如果 $\boldsymbol{\lambda}=(n-1,1)$, 则 $U_{\boldsymbol{\lambda}}$ 是 S_n 在 $\mathbf{C}^n$ 上由置换标准基的元得到的标准表示; 它可分解为 $\mathbf{1}\oplus V_{(n-1,1)}$, 其中 $\mathbf{1}$ 是 $\mathbf{C}^n$ 中由 $(1,\ldots,1)$ 生成的直线, 而 $V_{(n-1,1)}$ 是超平面 $\sum_{i=1}^n x_i=0$.
- 如果 $\boldsymbol{\lambda}=(1,\ldots,1)$, 则 $S_{\boldsymbol{\lambda}}=\{1\}$, 从而 $U_{(1,\ldots,1)}$ 是 S_n 的正则表示.

如同例子 $U_{(n-1,1)}$ 所指出的, 表示 $U_{\boldsymbol{\lambda}}$ 并不是不可约的, 但是它的不可约表示分解中出现了一个不会出现在 $U_{\boldsymbol{\mu}}, \boldsymbol{\mu}>\boldsymbol{\lambda}$ 中的唯一的不可约表示 $V_{\boldsymbol{\lambda}}$. 另外, 我们还可以给出 $V_{\boldsymbol{\lambda}}$ 的一个直接构造 (见后面).

[467] 2. 杨氏图及 S_n 的表示

设 $\boldsymbol{\lambda}=(\lambda_1,\ldots,\lambda_r)$ 是 n 的一个分拆, 以 $Y_{\boldsymbol{\lambda}}$ 记与 $\boldsymbol{\lambda}$ 相关的杨氏图: 这是 $n\times n$ 正方格的一个子集, 它由在第一行取前 λ_1 个格, 第二行取前 λ_2 个格, ……, 在第 r 行取前 λ_r 个格. 如果 $\boldsymbol{\lambda}^*=(\lambda_1^*,\ldots,\lambda_s^*)$ 是 n 的共轭于 $\boldsymbol{\lambda}$ 的分拆, 它由定义 λ_i^* 为那些 $\geqslant i$ 的 λ_j 的个数得到 (因此 $\lambda_1^*=r$, 而 $s=\lambda_1$), 于是 $Y_{\boldsymbol{\lambda}}$ 也可以有在第一列取前 λ_1^* 个格, 在第二列取前 λ_2^* 个格, ……. 特别地, $\boldsymbol{\lambda}$ 和 $\boldsymbol{\lambda}^*$ 的杨氏图相对于对角线对称.

表示 $V_{\boldsymbol{\lambda}}$ 可直接构造如下. 以数 1 到 n 填充进与 $\boldsymbol{\lambda}$ 相关的杨氏图 (从而得到了所谓的杨氏表格). 这让我们得到 S_n 的两个子群 A 和 B: A (分别地, B) 是保持这些行 (分别地, 列) 都整个不变的 $\{1,\ldots,n\}$ 的置换子群. 因此 $V_{\boldsymbol{\lambda}}$ 是 S_n 的正则表示 $\oplus_{\sigma\in S_n}\mathbf{C}e_\sigma$ 的子表示, 它由向量 $\sum_{a\in A,b\in B}\operatorname{sign}(b)e_{ab}$ 生成. 由 $\sum_{a\in A,b\in B}\operatorname{sign}(b)e_{ab}$ 生成的子空间依赖于杨氏表格, 但容易看出, 在同构范围内, 这样得到的表示并不依赖于它; 它只与分拆 $\boldsymbol{\lambda}$ 有关.

例如, 如果 $\boldsymbol{\lambda}=(1,\ldots,1)$, 则有 $A=\{1\}$, 而 $B=S_n$. 因此表示 $V_{\boldsymbol{\lambda}}$ 由 $v=\sum_{\sigma\in S_n}\operatorname{sign}(\sigma)e_\sigma$ 生成, 当 $g\in S_n$ 时由于有 $g\cdot v=\operatorname{sign}(g)v$ (不要忘了 $\operatorname{sign}(g)\in\{\pm1\}$), 这个表示是对应于 S_n 的线性特征标 sign 的一维表示. 更一般地, 由以上构造不难看出 $V_{\boldsymbol{\lambda}^*}=V_{\boldsymbol{\lambda}}\otimes\operatorname{sign}$.

$V_{\boldsymbol{\lambda}}$ 的维数由所谓的*角尺公式*给出. 如果 a 是 $\boldsymbol{\lambda}$ 的杨氏表格的一个格子, 顶点 a 的一个角尺 E_a 是位于与 a 同一行的右边的格子和与 a 同一列下面的格子 (包含 a) 的并, 长 $\lg(E_a)$ 是它包含的元的个数, 我们有

$$\dim V_{\boldsymbol{\lambda}}=\frac{n!}{\prod_{a\in Y_{\boldsymbol{\lambda}}}\lg(E_a)}.$$

习题 C.2.1. — 计算 S_3,S_4 和 S_5 的不可约表示的维数, 并将这些结果与习题 I.3.23, I.3.26 和 I.3.27 的进行比较.

3. S_n 的特征标

$U_{\boldsymbol{\lambda}}$ 和 $V_{\boldsymbol{\lambda}}$ 的特征标具有十分神奇的紧凑表达式: 如果 $\boldsymbol{\ell}=(\ell_1,\ldots,\ell_r)$ 和 $\boldsymbol{\lambda}=(\lambda_1,\ldots,\lambda_s)$, 则

$$\chi_{U_{\boldsymbol{\lambda}}}(C_{\boldsymbol{\ell}})=X_n^{\lambda_1}\ldots X_n^{\lambda_n}\text{ 在 }P_{\boldsymbol{\ell}}\text{ 中的系数},$$
$$\chi_{V_{\boldsymbol{\lambda}}}(C_{\boldsymbol{\ell}})=X_1^{\lambda_1+n-1}\cdots X_n^{\lambda_n}\text{ 在 }P_{\boldsymbol{\ell}}\cdot\prod_{i<j\leqslant n}(X_i-X_j)\text{ 中的系数},$$

其中 $P_{\boldsymbol{\ell}}(X_1,\ldots,X_n)=(X_1^{\ell_1}+\cdots+X_n^{\ell_1})\cdots(X_1^{\ell_r}+\cdots+X_n^{\ell_r})$, 而当 $s+1\leqslant i\leqslant n$ 时 $\lambda_i=0$. [468]

如果 $\boldsymbol{\mu}=(\mu_1,\ldots,\mu_s)$ 是 n 的一个分拆, 仍以 $\boldsymbol{\mu}$ 记满足当 $s+1\leqslant i\leqslant n$ 时 $\mu_i=0$ 的 $(\mu_1,\ldots,\mu_n)$. 定义*舒尔 (Schur) 多项式* $\mathrm{Sch}_{\boldsymbol{\mu}}$ 为

$$\mathrm{Sch}_{\boldsymbol{\mu}}(X_1,\ldots,X_n)=\frac{\det\begin{pmatrix}X_1^{\mu_1+n-1} & \ldots & X_n^{\mu_n+n-1}\\ \vdots & X_j^{\mu_j+n-i} & \vdots\\ X_1^{\mu_1} & \ldots & X_n^{\mu_n}\end{pmatrix}}{\det\begin{pmatrix}X_1^{n-1} & \ldots & X_n^{n-1}\\ \vdots & X_j^{n-i} & \vdots\\ 1 & \ldots & 1\end{pmatrix}}.$$

如果 $\boldsymbol{\lambda}=(\lambda_1,\ldots,\lambda_r)$ 是 n 的另一个分拆, 定义 Kostka 数 $K_{\boldsymbol{\mu},\boldsymbol{\lambda}}$ 为 $X_1^{\lambda_1}\cdots X_r^{\lambda_r}$ 在 $\mathrm{Sch}_{\boldsymbol{\mu}}(X_1,\ldots,X_n)$ 中的系数.

我们有 $U_{\boldsymbol{\lambda}}=\sum_{\boldsymbol{\mu}}K_{\boldsymbol{\mu},\boldsymbol{\lambda}}V_{\boldsymbol{\mu}}$, 且当 $\boldsymbol{\mu}<\boldsymbol{\lambda}$ 时 $K_{\boldsymbol{\mu},\boldsymbol{\lambda}}=0$, 而 $K_{\boldsymbol{\lambda},\boldsymbol{\lambda}}=1$, 因为可以证明 $V_{\boldsymbol{\lambda}}$ 对于 $\boldsymbol{\mu}>\boldsymbol{\lambda}$ 不出现在 $U_{\boldsymbol{\mu}}$ 中. 另外, 由于 $U_{(1,\ldots,1)}$ 是正则表示, 由此从推论 I. 2.23 和上面的公式得到 $\dim V_{\boldsymbol{\mu}}=K_{\boldsymbol{\mu},(1,\ldots,1)}$.

对于数 $K_{\boldsymbol{\mu},\boldsymbol{\lambda}}$ 还有一个组合式的解释: 它是填写 $\boldsymbol{\lambda}$ 的杨氏表格的如下的不同方式的个数: 数 1 填 λ_1 次, 数 2 填 λ_2 次, ……, 数 r 填 λ_r 次, 使每一行 (广泛意义上) 递增, 而每列严格递增.

利用以上对于 $V_{\boldsymbol{\mu}}$ 的维数公式可以得到 $\dim V_{\boldsymbol{\mu}}$ 是分拆 $\boldsymbol{\mu}$ 的其行与列均递增的杨氏表格的个数; 称一个这样的杨氏表格是标准的[2]. 这个组合式证明它与角尺公式相合并不是完全显然的.

C.3. $\mathbf{GL}_2(\mathbf{F})$ 的表示

1. 群 $\mathbf{GL}_2(\mathbf{F})$

设 $\mathbf{F}$ 是个基数为 q 的有限域. 于是存在一个素数 p 使得在 $\mathbf{F}$ 中 $p=0$, 这使得 $\mathbf{F}$ 是一个有限维的 $\mathbf{F}_p$-向量空间 (其中 $\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$), 从而 q 是 p 的一个幂.

[469] 设 $G=\mathbf{GL}_2(\mathbf{F})$ 为系数在 $\mathbf{F}$ 中的行列式非零的 2×2 矩阵的群. 如果 $g=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathbf{M}_2(\mathbf{F})$, 则 $g\in G$ 当且仅当此矩阵的列在 $\mathbf{F}$ 上线性无关, 这意味着第一个向量非零而第二个不在第一个生成的直线上. 由此得到 $|\mathbf{GL}_2(\mathbf{F})|=(q^2-1)(q^2-q)$.

在 $\mathbf{F}$ 有唯一的 2 次扩域 $\mathbf{K}$ (参看小词典的 8.7 小节). 如果 $p\neq 2$, 选取 $\Delta\in\mathbf{F}^*$ 在 $\mathbf{F}^*$ 不是一个平方元[3], 而 Δ 在 $\mathbf{K}$ 中有一个平方根 δ. 于是可以对 $z=x+\delta y$ 伴以一个矩阵 $C_z=\begin{pmatrix}x&\Delta y\\y&x\end{pmatrix}$, 它是在 $\mathbf{K}$ 上乘以 z 时在 $\mathbf{F}$ 上的基 $1,\delta$ 下的矩阵[4]. 直接的计算表明, 以 $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ 做共轭将 C_z 变成了 $C_{\bar z}$, 其中 $z=x+\delta y,\bar z=x-\delta y$.

---

[2] C. Schensted (1961) 建立了同样形式的杨氏表格偶对与置换之间的一个双射, 这便给出了在 S_n 情形时的 Burnside 公式 (推论 I.2.23 的 (ii)) 的一个组合证明 (mod 角尺公式).

[3] 如果 $p=2$, 因为 $X^2-\Delta$ 非不可约, 可做下面的一点修改: 选取 $\Delta\in\mathbf{F}$, 使它不在 $x\mapsto x^2+x$ 的像中, 而取 $\delta\in\mathbf{K}$ 满足 $\delta^2+\delta=\Delta$. 因此可对 $z=x+\delta y$ 伴以一个矩阵 $C_z=\begin{pmatrix}x&\Delta y\\y&x+y\end{pmatrix}$, 则是 $\mathbf{K}$ 在 $\mathbf{F}$ 上的基 $1,\delta$ 下乘以 z 的矩阵. 以 $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ 作共轭将 $C_z,z=x+\delta y$ 变成了 $C_{\bar z},\bar z=x+(\delta+1)y$.

[4] 注意其与复数的矩阵表示的类似性.

2. 构造 $\mathbf{GL}_2(\mathbf{F})$ 的表示

我们想要做出 G 的不可约表示的清单. 布饶尔定理 (定理 I.3.20) 证明了从子群的线性特征标的诱导可以得到它们. 另外, 由于不可约表示的维数通常相当小, 故我们的兴趣在于从可能最大的那些子群来做诱导. 下面的所有的表示均是在这种思考下得到的.

- *一维表示*. 如果 $\eta \in \widehat{\mathbf{F}^*}$ 是 $\mathbf{F}^*$ 的一个线性特征标, 我们可以与行列式运算造出一个 G 的线性特征标.

- Steinberg *群和它的扭变*. 以 $\mathbf{P}^1(\mathbf{F})$ 记 $\mathbf{F}^2$ 的向量直线的集合; 这是由 G 在上作用的 $q+1$ 个元的集合. 因此对应于它的是一个置换表示 $V_{\mathbf{P}^1(\mathbf{F})} = \oplus_{x\in\mathbf{P}^1(\mathbf{F})}\mathbf{C}e_x$, 因为由 $\sum_{x\in\mathbf{P}^1(\mathbf{F})} e_x$ 生成的直线在 G 下不动, 它不可能是不可约的. 以 St 记 G 在超平面 $\{\sum_{x\in\mathbf{P}^1(\mathbf{F})} \lambda_x e_x, \sum_{x\in\mathbf{P}^1(\mathbf{F})} \lambda_x = 0\}$ 上的表示. 这是一个 q 维的表示.

更一般地, 如果 $\eta \in \overline{\mathbf{F}^*}$, 我们可以考虑以 $\eta\circ\det$ 扭变 St 而得到表示 $\mathrm{St}\otimes(\eta\circ\det)$.

- *主列* (*principal séries*). 设 B 是 G 的博雷尔 (Borel) 子群; 它是上三角可逆矩阵的集合. 如果 $\eta_1, \eta_2 \in \widehat{\mathbf{F}^*}$ 为 $\mathbf{F}^*$ 的两个不同的线性表示, 以 $\eta_1\otimes\eta_2$ 记 B 的如下定义的线性表示

$$(\eta_1\otimes\eta_2)\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \eta_1(a)\eta_2(d).$$

如果 $\eta_1 \neq \eta_2$, 称表示 $\mathrm{Ind}_B^G \eta_1\otimes\eta_2$ 为*主列*[5]. [470]

- *其他的表示*. 如我们将看到的, 前面的这些表示都是不可约的, 但要填满 G 的不可约表示的列表还不足够. 以下的这些表示不是不可约的 (是由一个很小的子群诱导的), 然而却包含了我们所缺少的那些表示.

—设 $C \subset G$ 是 K^* 在 $z \mapsto C_z$ 下的像, 这是一个基数为 q^2-1 的 G 的子群[6]. 如果 $\eta \in \widehat{\mathbf{K}^*}$, 我们也可以利用从 K^* 到 C 上的同构 $z \mapsto C_z$ 将 η 看成是 C 的一个特征标, 因而可以考虑表示 $\mathrm{Ind}_C^G \eta$.

—设 $ZU \subset B$ 为仅具有一个特征值的矩阵的子群 (Z 在这里代表中心, 它是具有非零比率的位似态射的矩阵, 而 U 是对角线上为 1 的上三角矩阵的群; 这样一个矩阵是幂幺的). 固定 $\mathbf{F}$ 的一个非平凡线性特征标 $\psi \in \widehat{\mathbf{F}}$, 而如果 $\eta \in \widehat{\mathbf{F}^*}$ 是一个 $\mathbf{F}^*$ 的线性特征标, 以 $\eta\otimes\psi$ 记 ZU 的定义于下的线性特征标:

$$(\eta\otimes\psi)\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \eta(a)\psi(a^{-1}b).$$

我们将考虑表示 $\mathrm{Ind}_{ZU}^G \eta\otimes\psi$. 事实上, 我们感兴趣的是那些从 $\widehat{\mathbf{K}^*}$ 的一个元 η 出发而

---

[5] 读者可以证明 $\mathrm{Ind}_B^G \eta\otimes\eta = V_{\mathbf{P}^1(\mathbf{F})}\otimes(\eta\circ\det)$, 它解释了为什么我们对 $\eta_1 = \eta_2$ 不感兴趣.

[6] 这样一个子群是个*不可展的嘉当子群*, 不可展嘉当子群 (un sous-groupe de Cartan non déployé) 是共轭于对角矩阵子群的子群.

后限制到 $\mathbf{F}^*$ 的表示 (用同一记号表示此限制).

3. $\mathbf{GL}_2(\mathbf{F})$ 的共轭类

由于 $\mathbf{F}$ 有唯一的 2 次扩域, 在差一个可逆矩阵的共轭范围内, 系数在 $\mathbf{F}$ 中的 2×2 的矩阵的分类等同于转移成 $\mathbf{R}$ 上的分类. 有四种不同的类型:

- I 型: A 为标量, 因而形如 $a_x = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$, 其中 $x \in \mathbf{F}$.
- II 型: A 仅具有唯一的特征值 $x \in \mathbf{F}$, 但不是对角形的矩阵; 因而它共轭于 $b_x = \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}$.
- III 型: A 在 $\mathbf{F}$ 中有两个特征值 $x \neq y$, 因而共轭于 $b_{x,y} = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$, 它也共轭于 $b_{y,x}$.
- IV 型: A 在 $\mathbf{F}$ 中没有特征值, 因而在 K 中具有两个特征值 $z \neq \bar{z}$, 这时 A 共轭于 c_z 和 $c_{\bar{z}}$.

由于我们感兴趣的是 G 的共轭类, 应该只保留那些上面列出的可逆矩阵. 我们最后得到图 1 中的那些参量的列表.

[471]

	描述	基数
E_{I}	$\mathbf{F}^*$	$q-1$
E_{II}	$\mathbf{F}^*$	$q-1$
E_{III}	$\{(x,y) \in \mathbf{F}^* \times \mathbf{F}^*, x \neq y\}/(x,y) \sim (y,x)$	$\frac{1}{2}(q-1)(q-2)$
E_{IV}	$\{z \in \mathbf{K}^*, \bar{z} \neq z\}/\bar{z} \sim z$	$\frac{1}{2}q(q-1)$

图 1. $\mathbf{GL}_2(\mathbf{F})$ 的共轭类的参量

命题 C.3.1. — *图 2 是 $\mathbf{GL}_2(\mathbf{F})$ 的共轭类列表.*

证明　唯一不能从命题前面的讨论直接推出来的是如何确定每个类的基数. 按一般的方式, 如果 G 是个群, 而 $x \in G$, 那么 x 的共轭类是 x 在 G 的内共轭作用 $(g \cdot x = gxg^{-1})$ 下的轨道 O_x; 如果 Z_x 是 x 在 G 中的中心化子 (即 G 中与 x 交换的元的集合), 我们有 $O_x = G/Z_x$, 因此 $|O_x| = \frac{|G|}{|Z_x|}$. 问题因此化为确定与一个给定矩阵交换的可逆矩阵的集合. 然而如果 $A \in \mathbf{M}_2(\mathbf{F})$, 与 A 交换的 $M \in \mathbf{M}_2(\mathbf{F})$ 的矩阵的集合是:

- 如果 A 为标量, 则为整个 $\mathbf{M}_2(\mathbf{F})$.

型	个数	类	表示	基数
I	$q-1$	$a_x, x \in E_{\mathrm{I}}$	$A_x = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$	1
II	$q-1$	$b_x, x \in E_{\mathrm{II}}$	$B_x = \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}$	q^2-1
III	$\frac{(q-1)(q-2)}{2}$	$b_{x,y}, (x,y) \in E_{\mathrm{III}}$	$B_{x,y} = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$	$q(q+1)$
IV	$\frac{q^2-q}{2}$	$c_z, z = x+\delta y \in E_{\mathrm{IV}}$	$C_z = \begin{pmatrix} x & \Delta y \\ 0 & x \end{pmatrix}$	q^2-q

图 2. $\mathbf{GL}_2(\mathbf{F})$ 的共轭类

- 如果 A 不是标量, 则为由 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 和 A 生成的向量子空间[(7)].

由此讨论我们得到下面的结果:

- 全都与 A_x 交换, 故在 a_x 中只有唯一的元.
- 与 B_x 交换的矩阵具有 $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, a, b \in \mathbf{F}$ 的形式, 而这个矩阵可逆当且仅当 $a \neq 0$.

B_x 的中心化子因而具有基数 $q(q-1)$, 从而 b_x 的元的个数是 $\frac{(q^2-1)(q^2-q)}{q(q-1)} = q^2-1$.

- 如果 $x \neq y$, 那些与 $B_{x,y}$ 交换的矩阵是形如 $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, a, b \in \mathbf{F}$ 的元, 而这样的矩 [472]

阵可逆当且仅当 $a \neq 0$ 且 $b \neq 0$. $B_{x,y}$ 的中心化子因而具有基数 $(q-1)^2$, 从而 $b_{x,y}$ 中的元的个数等于 $\frac{(q^2-1)(q^2-q)}{(q-1)^2} = q(q+1)$.

- 如果 $z \in \mathbf{K} - \mathbf{F}$, 那么与 C_z 交换的矩阵形如 $C_{z'}, z' \in K$, 而此矩阵可逆当且仅当 $z' \neq 0$. 因此 C_z 的中心化子的基数等于 q^2-1, 那么, c_z 的元的个数是 $\frac{(q^2-1)(q^2-q)}{q^2-1} = q(q-1)$.

得到了结论. □

4. $\mathbf{GL}_2(\mathbf{F})$ 的特征标表

从现在开始假设 q 不是 2 的幂 (在 $p=2$ 的情形有一点小修改 (见脚注 3); 将其留作一个习题); G 的特征标以与 G 的共轭类平行的方式被赋予参数. 在图 3 中也有

[(7)]粗略的计算可证明, 如果 A 不是标量, 那么问题的解空间是 2 维的, 并因为 1 和 A 均与 A 交换且线性无关, 从而得到结论. 这个推理在二维情形是合理的, 但在任意维的情形要确定与一个矩阵交换最好要利用 §10 的 10.2 小节的观点.

被集合 $E_{\mathrm{I}}^*, E_{\mathrm{II}}^*, E_{\mathrm{III}}^*$ 和 E_{IV}^* 作为参数的 4 种类型.

	描述	基数
E_{I}^*	$\widehat{\mathbf{F}^*}$	$q-1$
E_{II}^*	$\widehat{\mathbf{F}^*}$	$q-1$
E_{III}^*	$\{(\eta_1,\eta_2)\in\widehat{\mathbf{F}^*}\times\widehat{\mathbf{F}^*}, \eta_1\neq\eta_2\}/(\eta_1,\eta_2)\sim(\eta_2,\eta_1)$	$\frac{1}{2}(q-1)(q-2)$
E_{IV}^*	$\{\eta\in\widehat{\mathbf{K}^*}, \eta^*\neq\eta\}/\eta^*\sim\eta$	$\frac{1}{2}q(q-1)$

图 3. $\mathbf{GL}_2(\mathbf{F})$ 的特征标的参量

在上面的表格中, η^* 代表线性特征标 $z\mapsto\eta(\bar{z})$, 其中 $\eta\in\widehat{\mathbf{K}^*}$.

定理 C.3.2. — 图 4 给出了 $\mathbf{GL}_2(\mathbf{F})$ 的特征标表.

[473] 证明 以 X 记出现在表 4 中的中心函数的集合 (即形如 $\alpha_\eta, \beta_\eta, \beta_{\eta_1,\eta_2}$ 或 γ_η 的). 由于对于 X 中的元和对于 G 的共轭类有同样的参数, 故只要证明对应于两个不同参数的这些 χ 也不同 (引理 C.3.6) 以及当 $\chi\in X$ 时有 $\chi\in\mathrm{Irr}(G)$ 就可以了. 为了证明第二个断言, 按照习题 I.2.22, 只要证明

- $\chi(1)\geqslant 0$(这是显然的),
- $\langle\chi,\chi\rangle=1$(这是引理 C.3.5 的目标),
- $\chi\in R_{\mathbf{Z}}(G)$(这是引理 C.3.4 的目标)

就可以了 (详细证明见后面). □

类型	I	II	III	IV
个数	$q-1$	$q-1$	$\frac{(q-1)(q-2)}{2}$	$\frac{q(q-1)}{2}$
特征标	$\alpha_\eta, \eta\in E_{\mathrm{I}}^*$	$\beta_\eta, \eta\in E_{\mathrm{II}}^*$	$\beta_{\eta_1,\eta_2}, (\eta_1,\eta_2)\in E_{\mathrm{III}}^*$	$\gamma_\eta, \eta\in E_{\mathrm{IV}}^*$
维数	1	q	$q+1$	$q-1$
a_x	$\eta(x)^2$	$q\eta(x)^2$	$(q+1)\eta_1\eta_2(x)$	$(q-1)\eta(x)$
b_x	$\eta(x)^2$	0	$\eta_1\eta_2(x)$	$-\eta(x)$
$b_{x,y}$	$\eta(xy)$	$\eta(xy)$	$\eta_1(x)\eta_2(y)+\eta_1(y)\eta_2(x)$	0
c_x	$\eta(z\bar{z})$	$-\eta(z\bar{z})$	0	$-(\eta(z)+\eta^*(z))$

图 4. $\mathbf{GL}_2(\mathbf{F})$ 的特征标表

注记 C.3.3. — (i) 将 (η_1,η_2) 换作 (η_2,η_1) 并不改变 III 型的列, 这证明了我们可以成功地转移到由等价关系 $(\eta_1,\eta_2)\sim(\eta_2,\eta_1)$ 所确定的商上.

(ii) 同样, 将 η 换作 η^* 不改变 IV 型的列 (因为若 $x \in \mathbf{F}^*$, 有 $\eta^*(x) = \eta(x)$), 这证明可以成功地转移到由等价关系 $\eta \sim \eta^*$ 所决定的商上.

5. 证明

引理 C.3.4. — (i) 如果 $\eta \in \widehat{\mathbf{F}^*}$, 则 $\alpha_\eta = \eta \circ \det$.

(ii) 如果 $\eta \in \widehat{\mathbf{F}^*}$, 则 β_η 是 $\mathrm{St} \otimes (\eta \circ \det)$ 的特征标.

(iii) 如果 $(\eta_1, \eta_2) \in E_{\mathrm{III}}$, 则 β_{η_1,η_2} 是 $\mathrm{Ind}_B^G \eta_1 \otimes \eta_2$ 的特征标.

(iv) 如果 $\eta \in E_{\mathrm{IV}}$, 则 $\gamma_\eta = \mathrm{Ind}_{ZU}^G \eta \otimes \psi - \mathrm{Ind}_C^G \eta$.

证明 (i) 直接可得. 为了证明其余的, 我们以 (e_1, e_2) 记 $\mathbf{F}^2$ 的标准基.

- 为证明 (ii), 应从计算 St 的特征标 χ_{St} 着手. 为此, 先计算置换表示 $V_{\mathbf{P}^1(\mathbf{F})}$ 的特征标 $\chi_{\mathbf{P}^1(\mathbf{F})}$, 这导致了 (§I.1 的 2.3 小节) 去计算 $g \in G$ 在 $\mathbf{P}^1(\mathbf{F})$ 上作用的不动点的个数. 由于这些不动点就是在 g 作用下 $\mathbf{F}^2$ 的特征值, 我们便可看出 A_x 的不动点的个数为 $q+1$, 而 B_x 的为 1(即直线 $\mathbf{F}e_1$), $B_{x,y}$ 的为 2(即直线 $\mathbf{F}e_1$ 和 $\mathbf{F}e_2$), 而 C_z 的为 0. 因为 $V_{\mathbf{P}^1(\mathbf{F})} = \mathrm{St} \oplus \mathbf{1}$, 故有 $\chi_{\mathrm{St}} = \chi_{\mathbf{P}^1(\mathbf{F})} - 1$, 从而 $\chi_{\mathrm{St}}(A_x) = q, \chi_{\mathrm{St}}(B_x) = 0, \chi_{\mathrm{St}}(B_{x,y}) = 1$ 以及 $\chi_{\mathrm{St}}(C_z) = -1$. (ii) 便由对特征标做 $\eta \circ \det$ 的扭变得到.
- 转到 (iii). 设 $\chi = \mathrm{Ind}_B^G \eta_1 \otimes \eta_2, \eta_1, \eta_2 \in \widehat{\mathbf{F}^*}$. 为计算 χ, 我们从定理 I.3.13 的公式开始:

$$\chi(g) = \frac{1}{|B|} \sum_{s \in G, sgs^{-1} \in B} \eta_1 \otimes \eta_2(sgs^{-1}).$$

◇ 由于 A_x 在 G 的中心中, 而它又包含在 B 中, 故对任意的 $s \in G$ 有 $sA_xs^{-1} \in B$ 和 $\eta_1 \otimes \eta_2(sA_xs^{-1}) = \eta_1\eta_2(x)$. 由此得到

$$\chi(A_x) = \frac{|G|}{|B|} \eta_1\eta_2(x) = (q+1)\eta_1\eta_2(x).$$

◇ 我们有 $sB_xs^{-1} \in B$ 当且仅当 $sB_xs^{-1}(e_1) \in \mathbf{F}e_1$, 于是当且仅当 $B_x(s^{-1}(e_1)) \in \mathbf{F}s^{-1}(e_1)$. 由于 $\mathbf{F}e_1$ 是 B_x 的唯一的一条特征直线, 这等价于说 $s^{-1}(e_1) \in \mathbf{F}e_1$, 因此等价于 $s \in B$. 因为当 $s \in B$ 时, $\eta_1 \otimes \eta_2(sB_xs^{-1}) = \eta_1\eta_2(x)$, 故得到了 [474]

$$\chi(B_x) = \frac{1}{|B|} \sum_{s \in B} \eta_1\eta_2(x) = \eta_1\eta_2(x).$$

◇ 同样证明 $sB_{x,y}s^{-1} \in B$ 当且仅当 $B_{x,y}(s^{-1}(e_1)) \in \mathbf{F}s^{-1}(e_1)$, 从而当且仅当 $s^{-1}(e_1) \in \mathbf{F}e_1$ 或者 $s^{-1}(e_1) \in \mathbf{F}e_2$. 像上面的证明那样, 第一个情形等价于 $s \in B$, 因此有 $\eta_1 \otimes \eta_2(sB_{x,y}s^{-1}) = \eta_1(y)\eta_2(x)$; 而第二个情形等价于 $s \in Bw$, 其中 $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, 因而有 $\eta_1 \otimes \eta_2(sB_{x,y}s^{-1}) = \eta_1(y)\eta_2(x)$. 由此得到

$$\chi(B_{x,y}) = \frac{1}{|B|}(\sum_{s \in B} \eta_1(x)\eta_2(y) + \sum_{s \in Bw} \eta_1(y)\eta_2(x)) = \eta_1(x)\eta_2(y) + \eta_1(y)\eta_2(x).$$

◇ 如果 $z \in \mathbf{K}^* - \mathbf{F}^*$, 则不存在任何 $s \in G$ 使得 $sC_zs^{-1} \in B$, 从而 $\chi(C_z) = 0$.

• 最后转向 (iv). 设 $\eta \in \widehat{\mathbf{K}^*}$, 且 χ_1 和 χ_2 分别是 $\mathrm{Ind}_{ZU}^G \eta \otimes \psi$ 和 $\mathrm{Ind}_C^G \eta$ 的特征标, 并令 $\chi = \chi_1 - \chi_2$. 根据定理 I.3.13, 有

$$\chi_1(g) = \frac{1}{|ZU|} \sum_{s \in G, sgs^{-1} \in ZU} \eta \otimes \psi(sgs^{-1}) \quad 和 \quad \chi_2(g) = \frac{1}{|C|} \sum_{s \in G, sgs^{-1} \in C} \eta(sgs^{-1}).$$

◇ 由于 $A_x \in ZU$ 和 $A_x \in C$, 像上面那样, 我们有

$$\chi_1(A_x) = \frac{|G|}{|ZU|}\eta(x) = (q^2 - 1)\eta(x) \quad 和 \quad \chi_2(A_x) = \frac{|G|}{|C|}\eta(x) = (q^2 - q)\eta(x),$$

因此 $\chi(A_x) = (q-1)\eta(x)$.

◇ 因为 ZU 中没有任何元共轭于 $B_{x,y}$ 或 C_z, 故 $\chi_1(B_{x,y}) = 0$ 和 $\chi(C_z) = 0$.

◇ 因为 C 中没有任何元共轭于 $B_{x,y}$ 或 B_x, 故 $\chi_2(B_{x,y}) = 0$ 和 $\chi_2(B_x) = 0$.

◇ 我们有 $ZU \subset B$. 然而在前面我们看到过, $sB_xs^{-1} \in B$ 蕴含了 $s \in B$. 加之, 由于 B_x 具有唯一的特征值, 那么 sB_xs^{-1} 亦如此, 故 $sB_xs^{-1} \in ZU$ 当且仅当 $s \in B$. 现在有

$$\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}^{-1} = \begin{pmatrix} \alpha x & \alpha + \beta x \\ 0 & \delta x \end{pmatrix} \begin{pmatrix} \alpha^{-1} & -\beta\alpha^{-1}\delta^{-1} \\ 0 & \delta^{-1} \end{pmatrix} = \begin{pmatrix} x & \alpha\delta^{-1} \\ 0 & x \end{pmatrix}.$$

由此得到

$$\chi_1(B_x) = \frac{1}{|ZU|} \sum_{\alpha,\delta \in \mathbf{F}^*, \beta \in \mathbf{F}} \eta(x)\psi(\alpha\delta^{-1}) = \frac{\eta(x)}{q-1} \sum_{\alpha,\delta \in \mathbf{F}^*} \psi(\alpha\delta^{-1}).$$

做变量变换 $\alpha' = \alpha\delta^{-1}, \delta' = \delta$, 并利用假设 ψ 非平凡而知道 $\sum_{\alpha' \in \mathbf{F}} \psi(\alpha') = 0$ 的事实 (群 $\mathbf{F}$ 的特征标 ϕ 和 $\mathbf{1}$ 的正交性), 最后得到

$$\chi_1(B_x) = \eta(x)(-\psi(0)) = -\eta(x) \quad 和 \quad \chi(B_x) = -\eta(x).$$

◇ 如果 $sC_zs^{-1} \in C$, 则 sC_zs^{-1} 等于 C_z 或者 $C_{\bar{z}}$ (C_z 的特征多项式等于 $X^2 - (z+\bar{z})X + z\bar{z}$, 因而也是 sC_zs^{-1} 的特征多项式). 如果 $sC_zs^{-1} = C_z$, 则 s 在 C_z 的中心化子中, 像我们见到过的那样 (命题 C.3.1 的证明中), 它等于 C; 如果 $sC_zs^{-1} = C_{\bar{z}}$, 则 $s\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} C_{\bar{z}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} s^{-1} = C_{\bar{z}}$, 因此 $s\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ 在 $C_{\bar{z}}$ 的中心化子中, 从而 $s \in C\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. 由此得到 [475]

$$\chi_2(C_z) = \frac{1}{|C|}(\sum_{s \in C} \eta(z) + \sum_{s \in C} \eta(\bar{z})) = \eta(z) + \eta^*(z) \quad 和 \quad \chi(C_z) = -(\eta(z) + \eta^*(z)).$$

于是得到结论. □

引理 C.3.5. — 如果 $\chi \in X$, 则 $\langle \chi, \chi \rangle = 1$.

证明 如果 ϕ 是 G 上的一个中心函数, 由共轭类表得到

$$|G|\langle \phi, \phi \rangle = \sum_{x \in \mathbf{F}^*} |\phi(a_x)|^2 + (q^2-1) \sum_{x \in \mathbf{F}^*} |\phi(b_x)|^2 + q(q+1) \sum_{\substack{(x,y)\in(\mathbf{F}^*)^2, x\neq y \\ \mathrm{mod}(x,y)\mapsto(y,x)}} |\phi(b_{x,y})|^2$$
$$+q(q-1) \sum_{\substack{z \in \mathbf{K}^* - \mathbf{F}^* \\ \mathrm{mod}\ z \mapsto \bar{z}}} |\phi(c_z)|^2.$$

我们应该证明, 当 ϕ 是一个出现在图 4 中的特征标时有 $|G|\langle \phi, \phi \rangle = (q^2-1)(q^2-q)$.

- 对于 $\eta \circ \det$ 类型的特征标, 因为我们处理的是自动为不可约的一维表示, 故无需证明什么.
- 注意到, 如果 ϕ 是表示 $\mathrm{St} \otimes (\eta \circ \det)$ 的特征标, 那么 $b_{x,y}$ 和 c_z 类所给出的贡献与 $\eta \circ \det$ 的是一样的. 因此只要证明 $\sum_{x \in \mathbf{F}^*} |\phi(a_x)|^2 + (q^2-1)\sum_{x \in \mathbf{F}^*} |\phi(b_x)|^2$ 在 $\phi = \eta \circ \det$ 的情形有同样的值就可以了, 这两个和的值为 $(q-1)q^2$.
- 在 $\phi = \beta_{\eta_1,\eta_2}$ 的情形, 其中 $\eta_1, \eta_2 \in \widehat{\mathbf{F}^*}$ 且 $\eta_1 \neq \eta_2$, 这个和的值为

$$(q-1)(q+1)^2 + (q-1)(q^2-1) + q(q+1) \sum_{\substack{(x,y)\in(\mathbf{F}^*)^2, x\neq y \\ \mathrm{mod}(x,y)\mapsto(y,x)}} |\eta_1(x)\eta_2(y) + \eta_2(x)\eta_1(y)|^2.$$

由于 $\bar{\eta}(a) = \eta(a)^{-1} = \eta(a^{-1})$, 故可将 $|\eta_1(x)\eta_2(y + +\eta_2(x)\eta_1(y)|^2$ 写成形如

$$2 + \eta_1(x)\eta_2(y)\overline{\eta_2(x)\eta_1(x)} + \overline{\eta_1(x)\eta_2(y)}\eta_2(x)\eta_1(y) = 2 + (\eta_1/\eta_2)(x/y) + (\eta_2/\eta_1)(y/x).$$

于是可取 $\sum |\eta_1(x)\eta_2(y) + \eta_2(x)\eta_1(y)|^2$ 为如下形式:

$$\begin{aligned}
&(q-1)(q-2) + \sum_{(x,y)\in(\mathbf{F}^*)^2, x\neq y} (\eta_1/\eta_2)(x/y) \\
&= (q-1)(q-2) + \sum_{(x,y)\in(\mathbf{F}^*)^2} (\eta_1/\eta_2)(x/y) - (q-1).
\end{aligned}$$

现在, 因为 $\eta_1 \neq \eta_2$, 故有 $\sum_{(x,y)\in(\mathbf{F}^*)^2} (\eta_1/\eta_2)(x/y) = 0$. 该和的值因此最后等于

$$\begin{aligned}
(q-1)(q+1)^2 + (q-1)(q^2-1) + q(q+1)(q-1)(q-3) &= (q^2-1)(q+1+q-1+q(q-3)) \\
&= (q^2-1)(q^2-q).
\end{aligned}$$

这就是我们要求的.

- 在 $\phi = \gamma_\eta$ 的情形, 其中 $\eta \in \widehat{\mathbf{K}^*}$ 且 $\eta \neq \eta^*$, 这个和的值是 [476]

$$(q-1)(q-1)^2 + (q-1)(q^2-1) + q(q-1) \sum_{z \in \mathbf{K}^* - \mathbf{F}^*, \mathrm{mod}\ z \mapsto \bar{z}} |\eta(z) + \eta^*(z)|^2.$$

与上面相同的计算 (利用了 $\eta^*(z)=\eta(\bar{z})$) 可将 $\sum_{z\in\mathbf{K}^*-\mathbf{F}^*,\mathrm{mod}\ z\mapsto\bar{z}}|\eta(z)+\eta^*(z)|^2$ 写为

$$q(q-1)+\sum_{z\in\mathbf{K}^*-\mathbf{F}^*}(\eta/\eta^*)(z)=q(q-1)+\sum_{z\in\mathbf{K}^*}(\eta/\eta^*)(z)-(q-1)$$

的形式, 并由于 $\eta\neq\eta^*$, 像上面一样有 $\sum_{z\in\mathbf{K}^*}(\eta/\eta^*)(z)=0$. 于是这个和的值最后等于

$$\begin{aligned}(q-1)(q-1)^2+(q-1)(q^2-1)+q(q-1)(q-1)^2&=(q-1)^2(q-1+q+1+q(q-1))\\&=(q-1)^2(q^2+q)=(q^2-1)(q^2-q).\end{aligned}$$

即为所求. □

引理 C.3.6. — 如果 χ 和 χ' 是 X 的两个使得 $\chi=\chi'$ 的元, 则 χ 和 χ' 的这些参数均相等.

证明　如果 $\chi=\chi'$, 特别有 $\chi(1)=\chi'(1)$, 这表明 χ 和 χ' 的型相同.

- 在 I 和 II 型, 要证明 χ 和 χ' 的参数均相同只需注意它在 $b_{x,y}$ 上的值就可以了.
- 为了处理 III 型的情形, 对于 $\widehat{\mathbf{F}^*}$ 中的元的偶对 (δ_1,δ_2), 我们以 $\mathbf{F}^*\times\mathbf{F}^*$ 的线性特征标 $\delta\otimes\delta_2$ 与其相伴, 它的定义为 $(\delta_1\otimes\delta_2)(x,y)=\delta_1(x)\delta_2(y)$. 如果 (η_1,η_2) 和 (η_1',η_2') 为 E_{III} 中的两个使得 $\beta_{\eta_1,\eta_2}=\beta_{\eta_1',\eta_2'}$ 的元, 并注意到它们在这些 $b_{x,y}$ 和 b_x 上的意思, 便能看出线性特征标 $\eta_1\otimes\eta_2,\eta_2\otimes\eta_1,\eta_1'\otimes\eta_2'$ 和 $\eta_2'\otimes\eta_1'$ 由以下的关系相联系:

$$\eta_1\otimes\eta_2+\eta_2\otimes\eta_1=\eta_1'\otimes\eta_2'+\eta_2'\otimes\eta_1'.$$

利用特征标的正交性, 证明了 $\eta_1\otimes\eta_2$ 等于 $\eta_1'\otimes\eta_2'$ 和 $\eta_2'\otimes\eta_1'$ 中的一个, 从而 E_{III} 中的两个元 (η_1,η_2) 和 (η_1',η_2') 相等.

- IV 型的情形可按统一方式处理. 如果 η_1 和 η_2 是 E_{IV} 中的两个使得 $\gamma_{\eta_1}=\gamma_{\eta_2}$ 的元, 于是注意到在这些 c_z 和 b_x 上的意思, 则看出在 $\mathbf{K}^*$ 上有 $\eta_1+\eta_1^*=\eta_2+\eta_2^*$. 利用特征标的正交性, 由此便得到 η_1 等于 η_2 或者 η_2^*, 从而 η_1 和 η_2 在 E_{IV} 中相等.

证完. □

附录 D. 单变元 p-adic 函数

在这一章里我们将描述一些经典概念在 p-adic 世界中的变化 ($\mathscr{C}^k$ 类函数, 解析函数积分, $\cdots\cdots$), 并在最后, 对库默尔 (Kummer) 发现的 ζ 函数在负整数上取值 (参看习题 VII.3.6) 间的同余关系的一个算术应用进行了讲述.

D.1. 实和 p-adic 泛函分析

本节致力于对在 $\mathbf{R}/\mathbf{Z}$ 上的经典泛函分析 (即研究周期函数的傅里叶展开的性质) 与在 $\mathbf{Z}_p$ 上的 p-adic 泛函分析 (马勒展开) 间进行比较. 结果是相当类似的, 但由于 p-adic 范数的超度量性, p-adic 方面的陈述常常要更加漂亮一点.

在下文中, 以 $c_k(\phi), k \in \mathbf{Z}$ 即 $\mathbf{R}/\mathbf{Z}$ 上一个函数的傅里叶系数 (在 $\mathbf{C}$ 中取值), 而以 $a_n(\phi), n \in \mathbf{N}$ 记一个 $\mathbf{Z}_p$ 上的函数的马勒系数 (在 $\mathbf{Q}_p$ 中取值).

从连续函数着手. 在 p-adic 情形, 我们有马勒定理 (小词典的定理 20.4), 其陈述如下.

定理 D.1.1. — (Mahler, 1958) 如果 $\phi \in \mathscr{C}(\mathbf{Z}_p)$, 则

(i) $\lim_{n\to+\infty} a_n(\phi) = 0$,

(ii) ϕ 是级数 $\sum_{n\in\mathbf{N}} a_n(\phi)\binom{x}{n}$ 在 $\mathscr{C}(\mathbf{Z}_p)$ 中的和; 特别地, 对于所有的 $x \in \mathbf{Z}_p$, 有 $\sum_{n\in\mathbf{N}} a_n(\phi)\binom{x}{n} = \phi(x)$,

(iii) 反之, 如果 $(a_n)_{n\in\mathbf{N}}$ 在 $+\infty$ 趋向 0, 则 $\sum_{n\in\mathbf{N}} a_n\binom{x}{n}$ 在 $\mathscr{C}(\mathbf{Z}_p, \mathbf{Q}_p)$ 中收敛于一个连续函数, 且其马勒系数等于 a_n.

在实的情形, 情况并不是非常清楚. (为了给出一个恰当的陈述, 应该考虑希尔伯特空间 $L^2(\mathbf{R}/\mathbf{Z})$ 而不是 $\mathscr{C}(\mathbf{R}/\mathbf{Z})$, 参看推论 II.2.7.)

定理 D.1.2. — (i) 如果 $\phi \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$, 则当 $|k| \to +\infty$ 时 $c_k(\phi) \to 0$.

[478] (ii) 如果 $\sum_{k\in\mathbf{Z}} |a_k(\phi)| < +\infty$, 则在 $\mathscr{C}(\mathbf{R}/\mathbf{Z})$ 中 $\sum_{k\in\mathbf{Z}} c_k(\phi)e^{2i\pi kx} \to \phi$. 特别地, 对所有的 $x \in \mathbf{R}/\mathbf{Z}$, 有 $\sum_{k\in\mathbf{Z}} c_k(\phi)e^{2i\pi kx} = \phi(x)$.

(iii) 如果 $\phi \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$, 则部分和序列 $\sum_{k=-n}^{n} c_k(\phi)e^{2i\pi kx}$ 几乎处处趋向 $\phi(x)$, 但存在 $\phi \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$ 使得对于 x 在 $\mathbf{R}/\mathbf{Z}$ 的一个不可数的稠子集上. 此序列不是有界的 (从而不趋向 $\phi(x)$).

(iv) 存在一个当 $|k| \to +\infty$ 时 $c_k \to 0$ 的序列 $(c_k)_{k\in\mathbf{Z}}$, 它不是任何一个连续函数的傅里叶系数.

证明 (i) 是性质 $\sum_{k\in\mathbf{Z}} |c_k(\phi)|^2 = \int_0^1 |\phi(t)|^2 dt$ (参看推论 II .2.7) 的结果, 而 (ii) 则是命题 IV.3.6 的内容, 又, 一个连续函数的傅里叶级数的几乎处处的收敛性是 Carleson(1965) 的一个难的结果, 但 (iii) 的其余部分和 (iv) 可以利用贝尔引理加以证明 (参看习题 II.3.17 和问题 H.5). □

这些断言在我们扩展了所考虑的函数的正则性后便成为了完全恒等的了. 回忆, 一个通项为 u_k 的序列 (其取值在一个具有范数 $\| \ \|$ 的域中) 是:

- 速降的是说, 如果当 $|k| \to +\infty$ 时对所有的 $N \in \mathbf{N}$ 有 $k^N\|u_k\| \to 0$.
- 按指数下降的是说, 存在 $r > 1$, 使得当 $|k| \to +\infty$ 时有 $r^{|k|}\|u_k\| \to 0$.

定理 D.1.3. — (i) $\phi \in \mathscr{C}(\mathbf{R}/Z)$ 属于 $\mathscr{C}^\infty$ 类当且仅当它的傅里叶系数是速降的.

(ii) $\phi \in \mathscr{C}(\mathbf{R}/\mathbf{Z})$ 是解析的当且仅当它的傅里叶系数是按指数下降的.

证明 利用一个函数的傅里叶系数和它的各阶导数之间的关系 (参看注记 IV.3.7) 立即得 (i) 的证明. (ii) 则是问题 H.9 的目标. □

在 p-adic 情形我们有下面的结果而它们中 (i)(分别地,(ii)) 的证明是 §D.2(分别地,§D.3) 的目标.

定理 D.1.4. — (i) $\phi \in \mathscr{C}(\mathbf{Z}_p)$ 一致地属于 $\mathscr{C}^\infty$ 当且仅当它的马勒系数的序列是速降的.

(ii) $\phi \in \mathscr{C}(\mathbf{Z}_p)$ 是局部解析的当且仅当它的马勒系数的序列是按指数下降的.

D.2. 一致可微的 k 重函数

1. $\mathscr{C}^k$ 类函数和 $\mathscr{C}_u^k$ 类函数

一个函数 $\phi : \mathbf{Z}_p \to \mathbf{Q}_p$ 在 $x_0 \in \mathbf{Z}_p$ 可微是指 $\frac{\phi(x_0+h)-\phi(x_0)}{h}$ 当 h 趋向 0 时有极限 (即它的导数). 称一个函数 1 阶可微是说它在每一个 $x_0 \in \mathbf{Z}_p$ 可微; 特别地, 一个 1 阶可微函数是连续的. 更一般地, 对 k 可归纳地定义 k 阶可微函数的概念: ϕ 为 k 阶可微的是指它的 $k-1$ 阶导数 $\phi^{(k-1)}$ 是 1 阶可微的. [479]

称 ϕ 属于 $\mathscr{C}^k$ 类是说它是 k 阶可微的, 并且其 k 阶导数连续. $\mathscr{C}^k$ 类的概念不太适合 p-adic 情形, 我们更愿意将其换作一致地属于 $\mathscr{C}^k$ 类的函数的概念 (简单地说成是属于 $\mathscr{C}_u^k$ 类): $\mathbf{Z}_p$ 上的函数 ϕ 属于 $\mathscr{C}_u^k$ 类是说, 在 $\mathbf{Z}_p \times (\mathbf{Z}_p - \{0\})^i$ $(0 \leqslant i \leqslant k)$ 上定义的函数 $\phi^{[i]}(x, h_1, \ldots, h_i)$ 可延拓为 $\mathbf{Z}_p^{i+1}$ 上的连续函数, 其中的 $\phi^{[i]}(x, h_1, \ldots, h_i)$ 在 $\mathbf{Z}_p \times (\mathbf{Z}_p - \{0\})^i$ $(0 \leqslant i \leqslant k)$ 上归纳地由公式: $\phi^{[0]}(x) = \phi(x)$ 和

$$\phi^{[i]}(x, h_1, \ldots, h_i) = \frac{1}{h_i}(\phi^{[i-1]}(x + h_i, h_1, \ldots, h_{i-1}) - \phi^{[i-1]}(x, h_1 \ldots, h_{i-1}))$$

定义.

一个 $\mathscr{C}_u^k$ 类函数属于 $\mathscr{C}^k$ 类, 并且其 k 阶导数由 $\phi^{(i)}(x) = \phi^{[i]}(x, 0, \ldots, 0)$ 给出.

注记 D.2.1. — (i) 在 $\mathbf{R}$ 上, 由于

$$\phi^{[i]}(x, h_1, \ldots, h_i) = \int_{[0,1]^i} \phi^{(i)}(x + t_1 h_1 + \cdots + t_i h_i) dt_1 \cdots dt_i,$$

故 $\mathscr{C}_u^k$ 的概念与 $\mathscr{C}^k$ 的重合.

(ii) 在 $\mathbf{Z}_p$ 上, 下面的例子证明这些概念此时没有任何意义. 按 p 为底的记法, $\mathbf{Z}_p$ 的每个元可以以唯一的方式写成 $\sum_{n=0}^{+\infty} p^n a_n(x)$ 形式, 其中 $a_n(x) \in \{0, \ldots, p-1\}$, 从而可以由公式 $\phi(x) = \sum_{n=0}^{+\infty} p^{2n} a_n(x)$ 定义一个函数 $\phi : \mathbf{Z}_p \to \mathbf{Z}_p$. 于是我们对于所有 $x, y \in \mathbf{Z}_p$ 有 $|\phi(x) - \phi(y)|_p = |x - y|_p^2$ (事实上, $|x - y|_p = p^{-k}$, 其中 k 是满足 $a_k(x) \neq a_k(y)$ 的最小整数, 这证明了 ϕ 在所有的点可微, 且其导数为 0(因此也属于 $\mathscr{C}^\infty$), 尽管 ϕ 在每个点上都不是常数. 另外, 如果 $(x, h_1, h_2) = (0, p^n, p^n)$, 则 $\phi^{[2]}(x, h_1, h_2) = 0$, 而如果 $(x, h_1, h_2) = ((p-1)p^n, p^n, p^n)$, 则 $\phi^{[2]}(x, h_1, h_2) = p - p^2$, 这证明了 $\phi^{[2]}$ 不可能连续地延拓到 $(0, 0, 0)$.

我们赋予 $\mathscr{C}_u^k(\mathbf{Z}_p)$ 一个自然范数 $\| \; \|_{\mathscr{C}_u^k}$, 其定义为

$$\|\phi\|_{\mathscr{C}_u^k} = \sup_{0 \leqslant i \leqslant k} \sup_{(x, h_1, \ldots, h_i) \in \mathbf{Z}_p^{i+1}} |\phi^{[i]}(x, h_1, \ldots, h_i)|_p.$$

因为连续函数的一致极限仍是连续的, 故 $\mathscr{C}_u^k(\mathbf{Z}_p)$ 完备, 从而是个 p-adic 巴拿赫空间.

定理 D.2.2. — (Barsky, 1973)

(i) $\phi \in \mathscr{C}_u^k$ 当且仅当通项为 $n^k |a_n(\phi)|_p$ 的序列趋向 0 且范数 $\sup_n (n+1)^k |a_n(\phi)|_p$ 等价于 $\|\phi\|_{\mathscr{C}_u^k}$.

(ii) ϕ 属于 $\mathscr{C}_u^\infty$ 当且仅当它的马勒系数的序列是速降的.

证明 一个函数属于 $\mathscr{C}_u^\infty$ 当且仅当对所有的 $k \in \mathbf{N}$ 它属于 $\mathscr{C}_u^k$ 类, 于是 (ii) 是 (i) 的推论. 至于 (i), 它是后面的引理 D.2.7 和 D.2.6 的推论 (用引理 D.2.6 可以证明序列 $n \mapsto (n+1)^k p^{-L(n,k)}$ 有界, 而引理 D.2.7 给出 $\|\phi\|_{\mathscr{C}_u^k} = \sup_{n \in \mathbf{N}} p^{L(n,k)} |a_n(\phi)|_p$). □ [480]

2. $\mathbf{Z}_p^m$ 上的连续函数

为了研究 $\mathscr{C}_u^k$ 类函数的马勒系数, 我们需要给出对 $\mathbf{Z}_p^m$ 上的连续函数一个描述 (比照于 $\mathscr{C}_u^k$ 类函数的定义, 它是十分自然的). 下面的结果表明了如何从 $\mathbf{Z}_p$ 上的连续函数的一族法正交基得到 $\mathbf{Z}_p^m$ 上的连续函数的一族法正交基. 这个完全类似于用 $L^2(\mathbf{R}/\mathbf{Z})$ 的正交基的函数去描述 $L^2((\mathbf{R}/\mathbf{Z})^m)$ 的法正交基的情形 [1]. 请读者将下面的陈述和它的证明与定理 IV.3.10 的陈述与证明进行比较.

命题 D.2.3. — 如果 $m \geqslant 1$, 则对于 $(k_1, \ldots, k_m) \in \mathbf{N}^m$, $\phi_{k_1,\ldots,k_m} = \binom{x_1}{k_1} \cdots \binom{x_m}{k_m}$ 构成了 $\mathscr{C}(\mathbf{Z}_p^m)$ 一族法正交基.

证明　只需证明它们的 mod p 约化构成 $\mathscr{C}(\mathbf{Z}_p^m, \mathbf{F}_p)$ 在 $\mathbf{F}_p$ 上的一族基就可以了. 为了证明它们是一个无关族, 可应用如下事实: 因为 $\binom{x}{k}$, $k \in \mathbf{N}$ 构成了 $\mathscr{C}(\mathbf{Z}_p)$ 的一族法正交基, 故 $\phi_k = \binom{x}{k}$, $k \in \mathbf{N}$ 为一个 mod p 的无关族. 直接进行归纳便从下面的引理得到了它们的无关性 (在引理中令 $K = \mathbf{F}_p, X = \mathbf{Z}_p$ 而 $Y = \mathbf{Z}_p^{m-1}$). □

引理 D.2.4. — 如果 K 为域, X 和 Y 为集合; 如果 $(f_i)_{i\in I}$ 和 $(g_j)_{j\in J}$ 分别是 K^X 和 K^Y 的两个无关族, 则 $(f_i \otimes g_j)_{(i,j)\in I\times J}$ 是 $K^{X\times Y}$ 中的无关族, 其中 $(f_i \otimes g_j)(x,y) = f_i(x)g_j(y)$.

证明　如果 $\sum \lambda_{i,j} f_i \otimes g_j$ 是在 $X \times Y$ 上恒等于 0 的一个线性组合 (只有有限个 $\lambda_{i,j}$ 不为零), 则对于所有的 $y \in Y$ 有 $\sum_{j\in J}(\sum_{i\in I} \lambda_{i,j} f_i(x)) g_j(y) = 0$. g_j 是无关族表明对于每个 $j \in J$ 和任意的 $x \in X$ 有 $\sum_{i\in I} \lambda_{i,j} f_i(x) = 0$. 因为这些 f_i 构成了无关族, 故而这些 $\lambda_{i,j}$ 全为 0. 得到结论. □

转到命题的证明. 剩下的还要证明这些 $\phi_{k_1,\ldots,k_m}$ 是个生成元族. 设 $\phi : \mathbf{Z}_p^m \to \mathbf{F}_p$ 连续. $\mathbf{F}_p$ 上的拓扑是离散的, 可以用平凡的距离 (当 $x \neq y$ 时 $d(x,y) = 1$), 且由于 $\mathbf{Z}_p^m$ 作为紧集的乘积是紧的, 故 ϕ 是一致连续的. 特别地, 这等于说, 存在 $N \in \mathbf{N}$ 使得 $\sup_{1\leqslant i\leqslant m} |x_i - y_i|_p \leqslant p^{-N}$ 蕴含了 $d(\phi(x), \phi(y)) < 1$(即 $\phi(x) = \phi(y)$); 换言之, 对于每个 $x \in \mathbf{Z}_p$, ϕ 在 $x + p^N \mathbf{Z}_p^m$ 上为常值; 因此它可写为

$$\phi = \sum_{0\leqslant r_1,\ldots,r_m \leqslant p^N - 1} \lambda_{r_1,\ldots,r_m} \mathbf{1}_{(r_1+p^N\mathbf{Z}_p)\times\cdots\times(r_m+p^N\mathbf{Z}_p)}$$

形式.

[481]　但是 $\mathbf{1}_{(r_1+p^N\mathbf{Z}_p)\times\cdots\times(r_m+p^N\mathbf{Z}_p)}(x) = \prod_{i=1}^m \mathbf{1}_{r_i+p^N\mathbf{Z}_p}(x_i)$, 而根据马勒定理, $\mathbf{1}_{r_i+p^N\mathbf{Z}_p}$ 则可以表达为这些 ϕ_k 的线性组合. 进一步要做的是展开所得到的表达式, 从而得到了 ϕ 是 $\phi_{k_1,\ldots,k_m}$ 的线性组合.

证完. □

注记 D.2.5. — (i) 由此命题得到: 每个 $\phi \in \mathscr{C}(\mathbf{Z}_p^m)$ 可以以唯一的方式写成 $\phi = \sum_{\boldsymbol{k}=(k_1,\ldots,k_m)\in\mathbf{N}^m} a_{\boldsymbol{k}}(\phi)\binom{x_1}{k_1}\cdots\binom{x_m}{k_m}$ 形式, 其中在无限远处 $a_{\boldsymbol{k}}(\phi) \to 0$, 于是

[1] 在第二种情形中, 多变量的函数空间是同一单变量的函数空间自身的完全张量积.

$\sum_{\boldsymbol{k}=(k_1,\cdots,k_m)\in\mathbf{N}^m} a_{\boldsymbol{k}}(\phi)\binom{x_1}{k_1}\cdots\binom{x_m}{k_m}$ 是 $\mathbf{Z}_p^m$ 上的一个连续函数, 而它的马勒系数为这些 $a_{\boldsymbol{k}}(\phi), \boldsymbol{k}\in\mathbf{N}^m$.

(ii) 如果 $\boldsymbol{n}=(n_1,\ldots,n_m)\in\mathbf{N}^m$, 则 $\binom{n_1}{k_1}\cdots\binom{n_m}{k_m}\in\mathbf{N}$, 并且除有限个 $\boldsymbol{k}$ 外全为 0. 由此得知 ϕ 在 $\mathbf{N}^m$ 上是 $a_{\boldsymbol{k}}(\phi), \boldsymbol{k}\in\mathbf{N}$ 的整数系数的线性组合. 反之, 像在 1 维的情形一样, 可以从 ϕ 在整数上的值定义马勒系数 $a_{\boldsymbol{k}}(\phi)$. 我们定义 "离散偏导数" 算子 $\partial_i^{[1]}$ 为

$$\partial_i^{[1]}\phi(x_1,\ldots,x_m)=\phi(x_1,\ldots,x_i+1,\ldots,x_m)-\phi(x_1,\ldots,x_i,\ldots,x_m),$$

并以 $\partial_i^{[k]}$ 记 k 个 $\partial_i^{[1]}$ 的复合. 那么, $a_{\boldsymbol{k}}(\phi)=\partial_1^{[k_1]}\cdots\partial_m^{[k_m]}\phi(0,\ldots,0)$. 这证明了 $a_{\boldsymbol{k}}(\phi)$ 是 $\phi(\boldsymbol{n}), \boldsymbol{n}\in\mathbf{N}^m$ 的整系数的线性组合.

3. $\mathscr{C}_u^k$ 类函数的马勒系数

令 $L(n,k)=\max\{v_p(n_1)+\cdots+v_p(n_i), i\leqslant k, n_1+\cdots+n_i\leqslant n, n_j\geqslant 1\}$.

引理 D.2.6. — *存在 $C_k>0$ 使得 $k\frac{\log n}{\log p}-C_k\leqslant L(n,k)\leqslant k\frac{\log n}{\log p}$.*

证明 如果 $n_i\leqslant n$, 则 $v_p(n_i)\leqslant\frac{\log n}{\log p}$, 从而 $L(n,k)\leqslant k\frac{\log n}{\log p}$. 另一方面, 如果 $k\leqslant p^r$, 且 $u=[\frac{\log n}{\log p}]$, 则可以取 $(n_1,\ldots,n_k)=(p^{u-r},\ldots,p^{u-r})$, 这表明 $L(n,k)\geqslant k(\frac{\log n}{\log p}-1-r)$, 因此有结论. □

引理 D.2.7. — *这些 $p^{L(n,k)}\binom{x}{n}$ 构成了 $\mathscr{C}_u^k(\mathbf{Z}_p)$ 的一个巴拿赫基.*

证明 令 $g_T(x)=(1+T)^x$. 我们有 $g_T(x)=\sum_{n\in\mathbf{N}}P_n(x)T^n$, 其中 $P_n(x)=\binom{x}{n}T^n$. 因此

$$\sum_{n\in\mathbf{N}}P_n^{[i]}(x,h_1,\ldots,h_k)=g_T^{[i]}(x,h_1,\ldots,h_k)=(1+T)^x\prod_{j=1}^{i}\frac{(1+T)^{h_j}-1}{h_j}.$$

将两端的 T 的 n 次项恒同并利用恒等式 $\frac{1}{h}\binom{h}{n}=\frac{1}{n}\binom{h-1}{n-1}$, 我们得到公式

$$P_n^{[i]}(x,h_1,\ldots,h_i)=\sum_{\substack{n_0+n_1+\cdots+n_i=n\\ n_1,\ldots,n_i\geqslant 1}}\frac{1}{n_1\cdots n_i}\binom{x}{n_0}\binom{h_1-1}{n_1-1}\cdots\binom{h_i-1}{n_i-1}.$$

设 $\phi\in\mathscr{C}_u^k(\mathbf{Z}_p)$, 并令 $g_i(x,h_1,\ldots,h_i)=\phi^{[i]}(x,h_1+1,\ldots,h_i+1)$. 由于对每个 $x\in\mathbf{Z}_p$, [482] $\phi(x)=\sum_{n\in\mathbf{N}}a_n(\phi)P_n(x)$, 从而从上面的公式推出

$$g_i(x,h_1,\ldots,h_i)=\sum_{n\in\mathbf{N}}\left(\sum_{\substack{n_0+n_1+\cdots+n_i=n\\ n_1,\ldots,n_i\geqslant 1}}\frac{a_n(\phi)}{n_1\cdots n_i}\binom{x}{n_0}\binom{h_1}{n_1-1}\cdots\binom{h_i}{n_i-1}\right),$$

从而 g_i 的马勒系数由

$$a_{n_0,n_1-1,\ldots,n_i-1}(g_i)=\frac{a_{n_0+\cdots+n_i}(\phi)}{n_1\cdots n_i}$$

给出.

如果 $i \leqslant k$. 因为 $\phi \in \mathscr{C}_u^k(\mathbf{Z}_p)$, 故 g_i 延拓成 $\mathbf{Z}_p^{i+1}$ 上的一个连续函数, 那么, 对于 $i+1$ 个变量时的马勒定理 (命题 D.2.3) 证明了通项为 $\frac{a_{n_0+\cdots+n_i}(\phi)}{n_1\cdots n_i}$ 的序列当 $(n_0,\ldots,n_i)$ 趋向无限时趋向 0.

反过来, 如果这个序列趋向 0, 并考虑到一个函数的马勒系数和它在整数上所取值之间的联系 (注记 D.2.5), 则级数

$$\sum_{n_0=0}^{+\infty}\sum_{n_1=1}^{+\infty}\cdots\sum_{n_i=1}^{+\infty}\frac{a_{n_0+\cdots+n_i}(\phi)}{n_1\cdots n_i}\binom{x}{n_0}\binom{h_1}{n_1-1}\cdots\binom{h_i}{n_i-1}$$

定义了 $\mathbf{Z}_p^{i+1}$ 上的一个连续函数, 且它在 $\mathbf{N}^{i+1}$ 上与 g_i 重合. 由于 $\mathbf{N}^{i+1}$ 在 $\mathbf{Z}_p\times(\mathbf{Z}_p-\{-1\})^i$ 中稠密, 故这证明了

- 上面的这个函数在 $\mathbf{Z}_p\times(\mathbf{Z}_p-\{-1\})^i$ 上等于 g_i,
- g_i, 从而 $\phi^{[i]}$ 可连续地延拓到 $\mathbf{Z}_p^{i+1}$ 上,
- $\|\phi^{[i]}\|_\infty=\|g_i\|_\infty=\sup_{n_0,\ldots,n_i}\frac{1}{|n_1\cdots n_i|_p}|a_{n_0+\cdots+n_i}|_p$.

总之, $\phi \in \mathscr{C}_u^k(\mathbf{Z}_p)$ 当且仅当在 $n=n_0+n_1+\cdots+n_i$ 趋向 $+\infty$ 时 $\frac{a_n(\phi)}{n_1\cdots n_i}$ 趋向 0, 并且

$$\|\phi\|_{\mathscr{C}_u^k}=\sup_{i\leqslant k}\sup_{n\in\mathbf{N}}\left(\sup_{\substack{n_0+n_1+\cdots+n_i=n\\ n_1,\ldots,n_i\geqslant 1}}\frac{|a_n(\phi)|_p}{|n_1\cdots n_i|_p}\right)=\sup_{n\in\mathbf{N}}p^{L(n,k)}|a_n(\phi)|_p.$$

故得到了结果. □

D.3. $\mathbf{Z}_p$ 上的局部解析函数

1. 解析函数

请读者将下面的陈述和它的证明与命题 V.1.10 的进行比较.

命题 D.3.1. — 设 $F=\sum_{n=0}^{+\infty}a_nT^n\in\mathbf{Q}_p[[T]]$, 满足当 $n\to+\infty$ 时 $a_n\to 0$.

(i) F 及其所有的导数在 $\mathbf{Z}_p$ 上收敛.

(ii) 如果 $z,z_0\in\mathbf{Z}_p$, 则 $F(z)=\sum_{k=0}^{+\infty}\frac{F^{(k)}(z_0)}{k!}(z-z_0)^k$, 其中的 $F^{(k)}(z_0)$ 代表级数 $F^{(k)}$ 在 z_0 的和.

(iii) 函数 $z\mapsto F(z)$ 在 $\mathbf{Z}_p$ 上属于 $\mathscr{C}^\infty$ 类, 且其在 z_0 的 k 阶导数是级数 $F^{(k)}$ 在 z_0 的值.

[483] (iv) 如果 $z_0\in\mathbf{Z}_p$, 则 $\frac{F^{(k)}(z_0)}{k!}\to 0$ 以及 $\sup_{k\in\mathbf{N}}|\frac{F^{(k)}(z_0)}{k!}|_p=\sup_{n\in\mathbf{N}}|a_n|_p$.

证明 我们有 $\frac{F^{(k)}(T)}{k!}=\sum_{n=0}^{+\infty}\binom{n+k}{k}a_{n+k}T^k$. 然而因为 $\binom{n+k}{k}\in\mathbf{N}$, 故有 $|\binom{n+k}{k}|_p\leqslant 1$, 从而当 $z\in\mathbf{Z}_p$(即当 $|z|_p\leqslant 1$) 时 $\binom{n+k}{k}a_{n+k}z^k\to 0$. 由此, 并由于 $|\ |_p$ 的超度量性, 推出了 $\mathbf{Z}_p$ 上 $\frac{F^{(k)}}{k!}$ 的级数收敛, (i) 得证.

现在, 如果 $z, z_0 \in \mathbf{Z}_p$, 则有

$$F(z)=\sum_{n=0}^{+\infty} a_n(z_0+(z-z_0))^n=\sum_{n=0}^{\infty} a_n\left(\sum_{k=0}^{\infty}\binom{n}{k} z_0^{n-k}(z-z_0)^k\right).$$

然而二重序列 $a_n\binom{n}{k}(z_0^k(z-z_0)^{n-k}$ 在无限远趋向 0, 由此, 并因 $|\,|_p$ 的超度量性, 让我们可以随意地对此级数重排序; 如果令 $n=m+k$, 这给了我们

$$F(z)=\sum_{k=0}^{+\infty}\left(\sum_{m=0}^{+\infty}\binom{m+k}{k} a_{m+k} z_0^m\right)(z-z_0)^k=\sum_{k=0}^{+\infty} \frac{F^{(k)}(z_0)}{k!}(z-z_0)^k.$$

于是得到了 (ii).

做变量变换 $z=z_0+h$, (ii) 让我们在 (iii) 的证明中可假设 $z_0=0$. 于是有

$$|\frac{F(h)-F(0)}{h}-F'(0)|_p=|h \sum_{n=2}^{+\infty} a_n h^{n-2}|_p \leqslant|h|_p \sup_{n \in \mathbf{N}}|a_n|_p,$$

其中 $h \in \mathbf{Z}_p$, 从而当 $h \rightarrow 0$ 时 $\frac{F(h)-F(0)}{h}-F'(0)$ 趋向 0, 这证明了 $z \mapsto F(z)$ 在 0 可微并且在 0 的导数为 $F'(0)$. 由此得到, $z \mapsto F(z)$ 在 $\mathbf{Z}_p$ 上可微且其在 z_0 的导数是级数 F' 在 z_0 的和. 直接的归纳便得到了 (iii).

最后, 如果 $z_0 \in \mathbf{Z}_p$, 则 $|\frac{F^{(k)}(z_0)}{k!}|_p \leqslant \sup_{n \in \mathbf{N}}|\binom{n+k}{k} a_{n+k} z_0^k|_p \leqslant \sup_{n \geqslant k}|a_n|_p$, 那么由于 $a_n \rightarrow 0$ 故有 $\frac{F^{(k)}(z_0)}{k!} \rightarrow 0$ 和 $\sup_{k \in \mathbf{N}}|\frac{F^{(k)}(z_0)}{k!}|_p \leqslant \sup_{n \in \mathbf{N}}|a_n|_P$. 要证明反向的不等式, 只要将前面的论证用到 $G(z)=\sum_{k=0}^{+\infty} \frac{F^{(k)}(z_0)}{k!} z^k$ 上即可: 我们有 $a_n=\frac{F^{(k)}(0)}{k!}=\frac{G^{(k)}(-z_0)}{k!}$. □

我们说 $\phi: \mathbf{Z}_p \rightarrow \mathbf{Q}_p$ 是解析的是指存在 $F=\sum_{n \in \mathbf{N}} b_n T^n \in \mathbf{Q}_p[[T]]$, 其中 $b_n \rightarrow 0$, 使得对所有的 $x \in \mathbf{Z}_p$ 有 $\phi(x)=F(x)$. 由命题 D.3.1 知, ϕ 在 $\mathbf{Z}_p$ 上属于 $\mathscr{C}^{\infty}$ 并且 $b_n=\frac{\phi^{(n)}(0)}{n!}$; 特别地, b_n 被 ϕ 决定, 从而可以记其为 $b_n(\phi)$.

我们赋予 $\mathbf{Z}_p$ 上的解析函数的空间 $\mathrm{An}(\mathbf{Z}_p)$ 一个范数 $\|\,\|_{\mathrm{An}}$, 定义为 $\|\phi\|_{\mathrm{An}}=\sup_{n \in \mathbf{N}}|b_n(\phi)|_p$. 根据命题 D.3.1, 也有 $\|\phi\|_{\mathrm{An}}=\sup_{n \in \mathbf{N}}|\frac{\phi^{(n)}(x)}{n!}|_p$, 其中对所有的 $x \in \mathbf{Z}_p$. 另外, 显然 $\phi \mapsto(b_n(\phi))_{n \in \mathbf{N}}$ 是从 $\mathrm{An}(\mathbf{Z}_p)$ 到 $\ell_0^{\infty}(\mathbf{N})$ 上的一个等距映射; 由此推出 $\mathrm{An}(\mathbf{Z}_p)$ 是一个 p-adic 巴拿赫空间, 其中对于 $n \in \mathbf{N}$ 的 x^n 构成了它的一个法正交基.

2. 局部解析函数 [484]

如果对于每个 $a \in \mathbf{Z}_p$ 存在 $h(a) \in \mathbf{N}$ 使得函数 $\phi: \mathbf{Z}_p \rightarrow \mathbf{Q}_p$ 满足 $x \mapsto \phi(a+p^{h(a)} x)$ 在 $\mathbf{Z}_p$ 上解析, 则称 ϕ 是*局部解析的*[(2)]. 根据命题 D.3.1, 如果 $x \mapsto \phi(a+p^{h(a)} x)$ 在 $\mathbf{Z}_p$ 是解析的, 那么对于每个 $b \in a+p^{h(a)} \mathbf{Z}_p$, $x \mapsto \phi(b+p^{h(a)} x)$ 也同样解析. 现

[(2)]尽管这个定义字面上等同于 $\mathbf{C}$ 上的全纯或解析函数的定义, 但因为这些函数不满足解析延拓的唯一性, 我们不采用解析函数的名字.

在, 由于 $\mathbf{Z}_p$ 为紧的, 故可从 $\mathbf{Z}_p$ 的开覆盖 $a+p^{h(a)}\mathbf{Z}_p$ 中抽出一个有限的子覆盖. 如果以 h 记那些出现在此有限覆盖中的 $h(a)$ 中的最小者, 那么, 对所有的 $b\in\mathbf{Z}_p$, $x\mapsto\phi(b+p^hx)$ 便在 $\mathbf{Z}_p$ 上解析; 换言之, 可以选取 $h(a)$ 与 $a\in\mathbf{Z}_p$ 无关.

以 $\mathrm{LA}(\mathbf{Z}_p)$ 记 $\mathbf{Z}_p$ 上的局部解析函数的空间, 并且, 如果 $h\in\mathbf{N}$, 令 $\mathrm{LA}_h(\mathbf{Z}_p)$ 是那些函数 $\phi:\mathbf{Z}_p\to\mathbf{Q}_p$ 的空间, 对于每个 $a\in\mathbf{Z}_p$ 它们使 $x\mapsto\phi(a+p^hx)$ 在 $\mathbf{Z}_p$ 上解析. 因此 $\mathrm{LA}_h(\mathbf{Z}_p)\subset\mathrm{LA}_{h+1}(\mathbf{Z}_p)$, 于是以上的讨论告诉我们 $\mathrm{LA}(\mathbf{Z}_p)=\cup_{h\in\mathbf{N}}\mathrm{LA}_h(\mathbf{Z}_p)$.

设 S 是 $\mathbf{Z}_p\mathrm{mod}\ p^h$ 的一个代表系. 于是可以将每个函数 $\phi:\mathbf{Z}_p\to\mathbf{Q}_p$ 以唯一的方式写成 $\sum_{j\in S}\mathbf{1}_{j+p^h\mathbf{Z}_p}\phi_j(\frac{x-j}{p^h})$ 形式, 其中 ϕ_j 是从 $\mathbf{Z}_p$ 到 $\mathbf{Q}_p$ 的函数 (显式地, ϕ_j 是 $x\mapsto\phi(j+p^hx)$ 在 $\mathbf{Z}_p$ 上的限制). 这是我们可以赋予 $\mathrm{LA}_h(\mathbf{Z}_p)$ 一个范数 $\|\ \|_{\mathrm{LA}_h}$: $\|\phi\|_{\mathrm{LA}_h}=\sup_{j\in S}\|\phi_j\|_{\mathrm{An}}$, 而命题 D.3.1 证明它不依赖于 S 的选取 (在后面, 我们将取 $S=\{-1,\ldots,-p^h\}$). 从构造知, 映射 $\phi\mapsto(\phi_j)_{j\in S}$ 是从 $\mathrm{LA}_h(\mathbf{Z}_p)$ 到 $\mathrm{An}(\mathbf{Z}_p)^{p^h}$ 上的一个等距映射, 这证明了 $\mathrm{LA}_h(\mathbf{Z}_p)$ 在范数 $\|\ \|_{\mathrm{LA}_h}$ 下是个 p-adic 巴拿赫空间.

定理 D.3.2. — (Amice, 1964)

(i) 对于 $n\in\mathbf{N}$ 的这些 $[\frac{n}{p^h}]!\binom{x}{n}$ 构成 $\mathrm{LA}_h(\mathbf{Z}_p)$ 的法正交基.

(ii) $\phi\in\mathrm{LA}(\mathbf{Z}_p)$ 当且仅当它的马勒系数的序列是按指数下降的.

证明 (ii) 是 (i) 的推论. 事实上, 如果 $\phi\in\mathrm{LA}(\mathbf{Z}_p)$, 由于 $\mathrm{LA}(Z_p)=\cup_{h\in\mathbf{N}}\mathrm{LA}_h(\mathbf{Z}_p)$, 故存在 $h\in\mathbf{N}$ 使得 $\phi\in\mathrm{LA}_h(\mathbf{Z}_p)$. 根据 (i), 这意味 $\phi=\sum_{n\in\mathbf{N}}b_n[\frac{n}{p^h}]!\binom{x}{n}$, 其中 $b_n\to0$. 于是有 $a_n(\phi)=b_n[\frac{n}{p^h}]!$; 从而存在 $C>0$ 使得 $|a_n(\phi)|_p\leqslant C|[\frac{n}{p^h}]!|_p$.

但是, 根据小词典的习题 1.4, 有 $v_p(m!)=\frac{m-S(m)}{p-1}$, 其中 $S(m)$ 是 m 的以 p 为底的记数法中的字码的和. 由于 m 最多有 $\frac{\log m}{\log p}$ 个字码非零, 并因为这些字码都 $\leqslant p-1$, 故得到上下界的估计:

$$\frac{m}{p-1}-\frac{\log m}{\log p}\leqslant v_p(m!)\leqslant\frac{m}{p-1}\quad 从而\quad p^{-m/(p-1)}\leqslant|m!|_p\leqslant mp^{-m/(p-1)}.$$

[485] 将此应用到 $m=[\frac{n}{p^h}]$, 则得到一个控制函数

$$|[\frac{n}{p^h}]!|_p\leqslant nC_hr_h^n,$$

其中 $r_h=p^{-1/(p-1)p^h}$, $C_h=\frac{p^{1/(p-1)}}{p^h}$, 从而知 $a_n(\phi)$ 按指数下降.

反之, 如果 $r>1$ 而 $r^n|a_n(\phi)|_p\to0$, 则存在 $h\in\mathbf{N}$ 使得 $r_h>r^{-1}$, 因此 $([\frac{n}{p^h}]!)^{-1}a_n(\phi)\to0$, 这表明 $\phi\in\mathrm{LA}_h(\mathbf{Z}_p)$. □

3. 局部解析函数空间的法正交基

我们已经证明了定理 D.3.2 的 (i) 蕴含了 (ii). 为了证明 (i), 我们将 $n\in\mathbf{N}$ 写成 $n=(m(n)+1)p^h-i(n)$ 的形式, 其中 $i(n)\in\{1,\ldots,p^h\}$, 而 $m(n)\in\mathbf{N}$(这种记数法唯一). 于是让 e_n 记函数 $x\mapsto\mathbf{1}_{n+p^h\mathbf{Z}_p}(x)(\frac{x+i(n)}{p^h})^{m(n)}$, 而以 g_n 记多项式 $[\frac{n}{p^h}]!\binom{x}{n}$. 我们的目的是要证明对于 $n\in\mathbf{N}$ 的 g_n 构成了 $\mathrm{LA}_h(\mathbf{Z}_p)$ 的法正交基. 为此, 我们将证明:

- 对于 $n \in \mathbf{N}$ 的这些 e_n 构成 $\mathrm{LA}_h(\mathbf{Z}_p)$ 的法正交基 (引理 D.3.3).
- g_n 属于 $\mathrm{LA}_h(\mathbf{Z}_p)$ 中的单位球 B_h.
- 以函数 $\bar{e}_n$, $n \leqslant (m+1)p^h-1$ 表达的约化 $\bar{g}_n$, $n \leqslant (m+1)p^h-1$ 的矩阵是可逆的 (像在引理 D.3.4 的证明前所解释的那样, 最后的这两个 • 都是该引理的推论).

根据命题 II.4.8, 第一个 • 蕴含了 $\bar{e}_n$, $n \in \mathbf{N}$ 构成了 B_h/pB_h 在 $\mathbf{F}_p$ 上的一个代数基. 而最后一个 • 则蕴含了对于 $\bar{g}_n$, $n \in \mathbf{N}$ 相同的结论, 根据命题 II.4.8 则蕴含了这些 g_n, $n \in \mathbf{N}$ 构成了 $\mathrm{LA}_h(\mathbf{Z}_p)$ 的法正交基.

引理 D.3.3. — e_n, $n \in \mathbf{N}$ 构成了 $\mathrm{LA}_h(\mathbf{Z}_p)$ 的一个法正交基. 更准确地, 如果 $\phi \in \mathrm{LA}_h(\mathbf{Z}_p)$, 且如果 $\phi_i = \phi(-i+p^h x)$, 则

- ϕ_i 在 $\mathbf{Z}_p$ 上解析, 因而 $\phi_i(x) = \sum_{m\in\mathbf{N}} \alpha_{i,m}x^n$, 其中 $\alpha_{i,m} \to 0$,
- $\phi = \sum_{i=1}^{p^h}\sum_{m\in\mathbf{N}} \alpha_{i,m}e_{(m+1)p^h-i} = \sum_{n\in\mathbf{N}} \alpha_{i(n),m(n)}e_n$,
- $\|\phi\|_{\mathrm{LA}_h} = \sup_{n\in\mathbf{N}} |\alpha_{i(n),m(n)}|_p$.

证明 这由恒等式 $\phi(x) = \sum_{i=1}^{p^h} \mathbf{1}_{-i+p^h\mathbf{Z}_p}(x)\phi_i(\frac{x+i}{p^h})$ 以及 $\|\phi\|_{\mathrm{LA}_h} = \sup_{1\leqslant i\leqslant p^h}\|\phi_i\|_{\mathrm{An}}$ 得到. □

如果 $j \in \{1,\ldots,p^h\}$, 令 $g_{n,j}$ 为由 $g_{n,j}(x) = g_n(-j+p^h x)$ 定义的多项式. 因此我们有

$$g_{n,j}(x) = [\frac{n}{p^h}]!\frac{1}{n!}\prod_{k=0}^{n-1}(-j-k+p^h x).$$

引理 D.3.4. — (i) $g_{n,j}$ 的系数在 $\mathbf{Z}_p$ 中.

(ii) 它的 mod p 约化 $\bar{g}_{n,j}$ 满足:

- 如果 $j > i(n)$, 则 $\bar{g}_{n,j} = 0$,
- 如果 $j = i(n)$, 则 $\deg(\bar{g}_{n,j}) = m(n)$, [486]
- 如果 $j < i(n)$, 则 $\deg(\bar{g}_{n,j}) \leqslant m(n)$.

这个引理让我们可以结束定理 D.3.2 的证明. 事实上, (i) 蕴含了 g_n 属于 $\mathrm{LA}_h(\mathbf{Z}_p)$ 的单位球. (ii) 可表述成, 对 $m \leqslant m(n)$ 存在 $\alpha_{j,m} \in \mathbf{F}_p$ 且当 $j > i(n)$ 时为 0, 使得 $\bar{g}_{n,j} = \sum_{m=0}^{m(n)} \alpha_{j,m}x^m$. 按照引理 D.3.3, 于是有 $\bar{g}_n = \sum_{m(k)\leqslant m(n)} \alpha_{i(k),m(k)}\bar{e}_k$. 现在, 如果 $n \leqslant (m+1)p^h-1$, 那么 $m(k) \leqslant m(n)$ 便意味着 $k \leqslant (m+1)p^h-1$. 由此得到, 对于 $n \leqslant (m+1)p^h-1$ 这些 $\bar{g}_n$ 可以借助 $\bar{e}_k$ 表达, 其中 $k \leqslant (m+1)p^h-1$. 以 M_m 记如此得到的矩阵. 那么, 引理的 (ii) 表明, 如果将矩阵 M_m 分成 $p^h \times p^h$ 大小的块, 便得到了上三角的分块矩阵, 而对角线上的每块是对角线上的元可逆的下三角矩阵 (这个可逆性来自当 $j = i(n)$ 时 $\deg(\bar{g}_{n,j}) = m(n)$). 因此矩阵 M_m 可逆, 这证明了引理 D.3.4 提供了证明定理 D.3.2 所需要的这些 •.

4. 引理 D.3.4 的证明

令 $K_{n,j}=\{k\leqslant n-1, v_p(j+k)\geqslant h\}$. 映射 $k\mapsto j+k$ 诱导了从 $K_{n,j}$ 到 $[j,j+n-1]=[0,j+n-1]-[0,j-1]$ 中被 p^h 整除的整数的集合上的一个双射, 于是有 $|K_{n,j}|=[\frac{j+n-1}{p^h}]-[\frac{j-1}{p^h}]$, 从而当 $j>i(n)$ 时有 $|K_{n,j}|=m(n)$ 而当 $j\leqslant i(n)$ 时 $|K_{n,j}|=m(n)$.

我们有 $g_{n,j}=c_{n,j}f_{n,j}$, 其中 $c_{n,j}\in\mathbf{Q}^*$, 而 $f_{n,j}=\prod_{k\in K_{n,j}}(x-\frac{j+k}{p^h})\prod_{k\notin K_{n,j}}(1-\frac{p^hx}{j+k})$ 是一个系数在 $\mathbf{Z}_p$ 中的多项式, 而它的 mod p 约化 $\bar{f}_{n,j}$ 是 $\prod_{k\in K_{n,j}}(x-\beta_k)$, 其中 $\beta_k\in\mathbf{F}_p$ 是 $\frac{j+k}{p^h}$ 的 mod p 约化. 由于 $\bar{f}_{n,j}$ 的次是 $K_{n,j}$ 的基数, 故此引理等价于下面的结果:

- 对所有的 j 有 $v_p(c_{n,j})\geqslant 0$,
- 如果 $j=i(n)$, 则 $v_p(c_{n,j})=0$,
- 如果 $j>i(n)$, 则 $v_p(c_{n,j})>0$.

将上面等式的常数项相等则得到了关系式 $c_{n,j}\prod_{k\in K_{n,j}}(\frac{-j-k}{p^h})=[\frac{n}{p^h}]!\frac{1}{n!}\prod_{k=0}^{n-1}(-j-k)$. 因此有

$$c_{n,j}=[\frac{n}{p^h}]!\frac{1}{n!}\prod_{k\in K_{n,j}}p^h\prod_{k\notin K_{n,j}}(-j-k).$$

$$v_p(c_{n,j})=v_p([\frac{n}{p^h}]!)-v_p(n!)+\sum_{0\leqslant k\leqslant n-1}\inf(v_p(j+k),h).$$

利用恒等式 $v_p(n!)-v_p([\frac{n}{p^h}]!)=\sum_{\ell=1}^{h}[\frac{n}{p^h}]$ (参看小词典的习题 1.4), 从而

$$\sum_{k=0}^{n-1}\inf(v_p(j+k),h)=\sum_{\ell=1}^{h}|\{k\leqslant n-1, v_p(j+k)\geqslant \ell\}|=\sum_{\ell=1}^{h}([\frac{n+j-1}{p^\ell}]-[\frac{j-1}{p^\ell}]),$$

[487] 由此便推出了公式

$$v_p(c_{n,j})=\sum_{\ell=1}^{h}\left([\frac{n+j-1}{p^\ell}]-[\frac{j-1}{p^\ell}]-[\frac{n}{p^\ell}]\right).$$

由于 $[x+y]\geqslant |x|+|y|$, 故这个和的每一项 $\geqslant 0$, 从而 $v_p(c_{n,j})\geqslant 0$. 第一个 • 得证.

为证明第二个, 我们利用公式 $-[\frac{-a}{b}]=[\frac{a-1}{b}]+1$, 它对于任意的 $a\in\mathbf{Z}$ 和 $b\in\mathbf{N}-\{0\}$ 均成立, 这给了我们

$$\begin{aligned}v_p(c_{n,i(n)})&=\sum_{\ell=1}^{h}\left([\frac{m(n)p^h-1}{p^\ell}]-[\frac{i(n)-1}{p^\ell}]-[\frac{m(n)p^h-i(n)}{p^\ell}]\right)\\&=\sum_{\ell=1}^{h}\left((m(n)p^{h-\ell}-1)+(1+[\frac{-i(n)}{p^\ell}])-(m(n)p^{h-\ell}+[\frac{-i(n)}{p^\ell}])\right)=0.\end{aligned}$$

最后, 为了证明第三个 •, 我们观察到当 $j > i(n)$ 时有 $[\frac{n+j-1}{p^h}] - [\frac{j-1}{p^h}] - [\frac{n}{p^h}] = 1$, 故 $v_p(c_{n,j}) \geqslant 1$.

完成证明.

D.4. p-adic ζ 函数

库默尔在他的关于费马定理的工作中 (参看第 VII 章的脚注 9) 发现了 ζ 函数在负整数上的值之间的 mod p^n 的同余关系, 如果思考一下, 就会发现它是非常有趣的: ζ 函数是由在负整数上并不收敛的级数定义的; 我们解析地延拓它 (这样的一个延拓的存在性多少有点神秘感), 我们发现在负整数上的这些值是些有理数而且, 锦上添花似的, 对于每个素数 p 这些有理数更具有突出的 p-adic 性质.

这些库默尔同余关系被 Kubota 和 Leopoldt(1964) 重新解释为 ζ 函数 $n \mapsto \zeta(-n)$ 的 p-adic 连续性的一个性质, 它将这些同余关系引到了 p-adic ζ 函数的构造方面.

定理 D.4.1. — 如果 $i \in \mathbf{Z}/(p-1)\mathbf{Z}$, 则存在一个唯一的函数 $\zeta_{p,i}$, 它当 $i \neq 1$(分别地, $i = 1$) 时在 $\mathbf{Z}_p$(分别地, $\mathbf{Z}_p - \{1\}$) 上连续, 并使得对满足 $-n \equiv i \bmod p-1$ 的 $n \in \mathbf{N}$ 有 $\zeta_{p,i}(-n) = (1-p^n)\zeta(-n)$.

注记 D.4.2. — (i) 如我们将看到的, $n \mapsto \zeta(-n)$ 的连续性是 $n \mapsto x^n$ 连续性的推论, 其中 $x \in \mathbf{Z}_p^*$.

(ii) 如果 $i \in \{1, \ldots, p-1\}$, 则满足 $-n \equiv i$ 的 $n \in \mathbf{N}$ 的集合是 $\mathbf{N}$ 在 $x \mapsto i-(p-1)(x+1)$ 下的像, 而由于 $\mathbf{N}$ 在 $\mathbf{Z}_p$ 中稠密, 且 $p-1 \in \mathbf{Z}_p^*$, 于是这个集合也在 $\mathbf{Z}_p$ 中稠密. 由此推出了 $\zeta_{p,i}$ 的唯一性; 相反地, 它的存在性则完全不是自动成立的, 多少有点出乎意料. 称函数 $\zeta_{p,i}$ 为 p-adic ζ 函数的第 i 个分支. 如果 i 为偶数且 $p \neq 2$, [488] 则由于当 $n \geqslant 2$ 为偶数时有 $\zeta(-n) = 0$, 故此时 $\zeta_{p,i}$ 恒为 0.

(iii) p-adic ζ 函数的零点 (不同于黎曼 ζ 函数的零点 ······) 已有很好的了解: 它们是"主猜想"的目标, 并已为马祖尔 (Mazur) 和怀尔斯 (Wiles)(1984) 所证明.

1. p-adic 积分

$\mathbf{Z}_p$ 上的一个测度 μ 是 $\mathscr{C}(\mathbf{Z}_p)$ 上的一个连续线性形式. 我们将 $\mu(\phi)$ 写成更富含义的形式:$\int_{\mathbf{Z}_p} \phi(x)\mu(x)$ 或者简单地写为 $\int_{\mathbf{Z}_p} \phi\mu$.

如果 μ 是 $\mathbf{Z}_p$ 上的一个测度, 以 $\|\mu\|_\infty$ 表示将 μ 作为算子时的范数, 就是说, 对于 $\|\phi\|_\infty \leqslant 1$ 的 $|\int_{\mathbf{Z}_p} \phi\mu|_p$ 的上确界.

- 以 $\mu(a+p^n\mathbf{Z}_p)$ 记 $a+p^n\mathbf{Z}_p$ 的测度 (即积分 $\int_{\mathbf{Z}_p} \mathbf{1}_{a+p^n\mathbf{Z}_p}\mu$).
- 由于 $a+p^n\mathbf{Z}_p$ 是 $a+jp^n+p^{n+1}\mathbf{Z}_p$, $0 \leqslant j \leqslant p-1$ 的不交并, 故有 $\mu(a+p^n\mathbf{Z}_p) = \sum_{j=0}^{p-1} \mu(a+jp^n+p^{n+1}\mathbf{Z}_p)$.
- 由于 $\|\mathbf{1}_{a+p^n\mathbf{Z}_p}\|_\infty = 1$, 故这些 $\mu(a+p^n\mathbf{Z}_p)$ 有界 (我们有 $|\mu(a+p^n\mathbf{Z}_p)| \leqslant \|\mu\|_\infty$).

如果利用 $\phi \in \mathscr{C}(\mathbf{Z}_p)$ 是 $\sum_{a=0}^{p^n-1}\phi(a)\mathbf{1}_{a+p^n\mathbf{Z}_p}$ 在 $\mathscr{C}(\mathbf{Z}_p)$ 的极限这个事实 (参看小词典的习题 20.6 的 (v) 的解) 和 μ 的连续性, 则得到公式

$$\int_{\mathbf{Z}_p}\phi\mu = \lim_{n\to+\infty}\sum_{a=0}^{p^{n-1}-1}\phi(a)\mu(a+p^n\mathbf{Z}_p),$$

这极像一个黎曼和.

注记 D.4.3. — (i) 反过来, 如果已知对于 $a \in \mathbf{Z}_p$ 和 $n \in \mathbf{N}$ 的 $\mathbf{Q}_p$ 中的一个族 $\mu(a+p^n\mathbf{Z}_p)$, 它满足以下条件:

- 对于 $v_p(a-b) \geqslant n$ 有 $\mu(a+p^n\mathbf{Z}_p) = \mu(b+p^n\mathbf{Z}_p)$,
- $\mu(a+p^n\mathbf{Z}_p) = \sum_{j=0}^{p-1}\mu(a+jp^n+p^{n+1}\mathbf{Z}_p)$,
- 对于任意的 $a \in \mathbf{Z}_p$ 和 $n \in \mathbf{N}$, 存在 $C \in \mathbf{R}$ 使得 $|\mu(a+p^n\mathbf{Z}_p)| \leqslant C$.

于是, 头两个条件可以让 μ 扩张为 $\mathbf{Z}_p$ 上的局部常值函数的空间 $\mathrm{LC}(\mathbf{Z}_p)$ 上的一个线性形式, 而第三个条件表明 $|\mu(\phi)|_p \leqslant C\|\phi\|_\infty$, 从而可以 (参看小词典的 17.2 小节) 连续地将 μ 扩张到 $\mathscr{C}(\mathbf{Z}_p)$.

(ii) 在 p-adic 情形没有哈尔测度, 因而没有一个标准的方法去对一个函数给出一个测度. 事实上, 一个在 $\mathbf{Z}_p$ 中平移下不变的测度 μ 应该满足 $\mu(a+p^n\mathbf{Z}_p) = \frac{1}{p^n}\mu(\mathbf{Z}_p)$, 因而 $|\mu(a+p^n\mathbf{Z}_p)|_p = p^n|\mu(\mathbf{Z}_p)|_p$, 其中 $a \in \mathbf{Z}_p$ 和 $n \in \mathbf{N}$. 但这是不可能的, 除非 $\mu(\mathbf{Z}_p) = 0$(从而 $\mu = 0$): 因为这些 $\mu(a+p^n\mathbf{Z}_p)$ 应该按范数 $\|\mu\|_\infty$ 有界.

对于一个测度 μ, 我们可以相应地伴随一个形式幂级数 $\mathscr{A}_\mu(T) = \sum_{n=0}^{+\infty}T^n\int_{\mathbf{Z}_p}\binom{x}{n}\mu(x)$ 并称其为 μ 的阿米斯变换. 这是傅里叶变换的 p-adic 类比: 因为形式地 $(1+T)^x = \sum_{n=0}^{+\infty}\binom{x}{n}T^n$ 故有 $\mathscr{A}_\mu(T) = \int_{\mathbf{Z}_p}(1+T)^x\mu(x)$, 因而可以将 T 看为 $e^{2i\pi}-1$ 的一个 p-adic 类比 (尽管 $e^{2i\pi x}$ 不总等于 1, 但在实数世界里它有着喜欢为零的坏口味 $\cdots\cdots$). [489]

定理 D.4.4. — $\mu \mapsto \mathscr{A}_\mu$ 是从具有范数 $\|\ \|_\infty$ 的测度的空间到具有有界系数的形式级数的空间的一个等距映射, 其中后者上的范数是其系数的范数的上确界.

证明　由于这些 $\binom{x}{n}$ 构成了 $\mathscr{C}(\mathbf{Z}_p)$ 的一族法正交基, 于是此定理是命题 II.4.9 的特殊情形. 显式地, 相伴于 $(b_n)_{n\in\mathbf{N}}$ 有界的形式级数 $\sum_{n\in\mathbf{N}}b_nT^n$ 的逆映射的像, 当 ϕ 是 $\mathbf{Z}_p$ 上的一个连续函数时, 是由 $\mu(\phi) = \sum_{n=0}^{+\infty}b_na_n(\phi)$ 定义的测度 μ. □

如果 $z \in \mathbf{C}$ 满足 $|z-1|_p > 0$, 则 $(z-1)^n \to 0$, 因而级数 $\phi_z(x) = \sum_{n=0}^{+\infty}\binom{x}{n}(z-1)^n$ 一致收敛, 于是定义了在 $\mathbf{Z}_p$ 上在 $\mathbf{C}_p$ 上取值的连续函数 $x \mapsto \phi_z(x)$(如果 $z \in \mathbf{Q}_p$, 这个函数则取值在 $\mathbf{Q}_p$ 中). 另一方面, 如果 $k \in \mathbf{N}$, 我们有 $\phi_z(k) = z^k$, 这让我们可以以更愉悦的方式将函数 $x \mapsto \phi_z(x)$ 记为 $x \mapsto z^x$. 于是对任意的 $x, y \in \mathbf{Z}_p$ 有 $z^{x+y} = z^xz^y$: 因为这个公式对 $x, y \in \mathbf{N}$ 成立, 而且 $\mathbf{N}^2$ 在 $\mathbf{Z}_p^2$ 中稠密.

特别地, 可将此用于 $z \in \mu_{p^n}$ 的情形 (参看习题 20.3). 因此对任意的 $k \in \mathbf{N}$ 有 $z^{x+p^nk} = z^x$, 于是当 $y \in x+p^n\mathbf{Z}_p$ 时 $z^x = z^y$, 这表明函数 $x \mapsto z^x$ 是局部常值的.

如果 μ 是 $\mathbf{Z}_p$ 上的一个测度, 则按照公式 $\int_{\mathbf{Z}_p}\phi\mu=\lim_{n\to+\infty}\sum_{a=0}^{p^n-1}\phi(a)\mu(a+p^n\mathbf{Z}_p)$(它的收敛性的证明, 可像在取值在 $\mathbf{Q}_p$ 的函数的情形那样, 利用 ϕ 的一致收敛性) 将 μ 扩张成在 $\mathbf{Z}_p$ 上的但取值在 $\mathbf{C}_p$ 的连续函数的空间 $\mathscr{C}(\mathbf{Z}_p,\mathbf{C}_p)$ 上的一个连续函数. 下面的引理证明了恒等式 $\mathscr{A}_\mu(T)=\int_{\mathbf{Z}_p}(1+T)^x\mu(x)$ 不只是形式的了.

引理 D.4.5. — 如果 $|z|_p<1$, 则 $\int_{\mathbf{Z}_p}(1+z)^x\mu(x)=\mathscr{A}_\mu(z)$.

证明　函数 $x\mapsto\sum_{n=0}^{N}\binom{x}{n}z^n$ 的序列在 $\mathbf{Z}_p$ 上一致收敛于 $x\mapsto(1+z)^x$(余项按范数 $\|\ \|_\infty$ 小于 $|z|_p^{n+1}$); 因此可以交换积分与求和, 从而得到结果. □

推论 D.4.6. — 如果 $i\in\mathbf{Z}_p$ 且 $n\in\mathbf{N}$, 则 $\mu(i+p^n\mathbf{Z}_p)=\frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}}\eta^{-i}\mathscr{A}_\mu(\eta-1)$.

证明　我们有

$$\sum_{\eta\in\boldsymbol{\mu}_{p^n}}\eta^x=\begin{cases}p^n, & \text{如果 } x\in p^n\mathbf{Z}_p,\\ 0, & \text{其他},\end{cases}$$

从而 $i+p^n\mathbf{Z}_p$ 的特征函数是 $\frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}}\eta^{x-i}$. 于是可以利用引理 D.4.5 得到结论. □

2. 测度 μ_a

[490]

在后文中 a 总表示一个 $\geqslant 2$ 且与 p 互素的整数. 我们可以将命题 VII.2.6 应用到函数

$$f_a(t)=\frac{1}{e^t-1}-\frac{a}{e^{at}-1},$$

它在 $\mathbf{R}_+$ 上属于 $\mathscr{C}^\infty$(我们以设法避开了在 0 的极点), 并且它及其所有阶导数在无限远处速降. 由于当 $\mathrm{Re}(s)>1$ 时有

$$\frac{1}{\Gamma(s)}\int_0^{+\infty}f_a(t)t^s\frac{dt}{t}=\frac{1-a^{1-s}}{\Gamma(s)}\int_0^{+\infty}\frac{1}{e^t-1}t^s\frac{dt}{t}=(1-a^{1-s})\zeta(s),$$

故对于 $\zeta(s)$ 在负整数上的我们得到如下公式:

引理 D.4.7. — 如果 $n\in\mathbf{N}$, 则 $(1-a^{1+n})\zeta(-n)=(-1)^nf_a^{(n)}(0)$.

命题 D.4.8. — 在 $\mathbf{Z}_p$ 上存在 (唯一的) 一个测度 μ_a 使得, 对于所有的 $n\in\mathbf{N}$ 有 $\int_{\mathbf{Z}_p}x^n\mu_a=(-1)^n(1-a^{1+n})\zeta(-n)$.

证明　μ_a 的唯一性来自 $\int_{\mathbf{Z}_p}x^n\mu_a$ 对于所有 n 时的了解, 这等价于 $\int_{\mathbf{Z}_p}\binom{x}{n}\mu_a$ 对所有当 $n\in\mathbf{N}$ 时的了解, 从而根据定理 D.4.4, 等价于 μ_a 的阿米斯变换.

令 $F_a(T)=\frac{1}{T}-\frac{a}{(1+T)^a-1}$, 于是 $F_a(e^t-1)=f_a(t)$ (作为对 t 的形式级数). 可将 $(1+T)^a-1$ 写成 $aT(1+Tg(T))$ 的形式, 其中 $g(T)=\sum_{n\geqslant2}\frac{1}{a}\binom{a}{n}T^{n-2}$, 由于 a 与 p 互素从而在 $\mathbf{Z}_p$ 中可逆, 属于 $\mathbf{Z}_p[T]$. 由此得到

$$F_a(T)=\frac{1}{T}-\frac{a}{(1+T)^a-1}=\sum_{n=1}^{+\infty}(-T)^{n-1}g^n\in\mathbf{Z}_p[[T]],$$

且因为 F_a 的系数整体有界, 从而 F_a 是某个测度 μ_a 的阿米斯变换. 现在, $\int_{\mathbf{Z}_p} x^n\mu_a$ 是形式级数 $\mathscr{L}(t)=\int_{\mathbf{Z}_p} e^{tx}\mu_a$ 在 $t=0$ 的 n 阶导数. 然而 $e^{tx}=(1+(e^t-1))^x$, 因此 $\mathscr{L}(t)=F_a(e^t-1)=f_a(t)$. 故从引理 D.4.7 得到 $\int_{\mathbf{Z}_p} x^n\mu_a=(-1)^n(1-a^{1+n})\zeta(-n)$, 命题得证. □

习题 D.4.9. — 证明如果 $n_1,n_2\geqslant k$ 且 $n_1\equiv n_2 \bmod (p-1)p^{k-1}$, 则 $(1-a^{1+n_1})\zeta(-n_1)\equiv(1-a^{1+n_2})\zeta(-n_2) \bmod p^k$. (证明 $\|x^{n_1}-x^{n_2}\|_\infty\leqslant p^{-k}$ 和 $\|\mu_a\|_\infty\leqslant 1$.)

3. 函数 $n\mapsto x^n$ 的连续性

如果 $x\in\mathbf{Z}_p$, 并不总存在连续函数 $s\mapsto x^s$ 使得对所有的 $n\in\mathbf{N}$, 它在 $s=n$ 取值 x^n, 但可给出一个多值函数, 它具有由 $\mathbf{Z}/(p-1)\mathbf{Z}$ 作为指标的分支, 并起着 x^s 的作用 (参看命题 D.4.13)

引理 D.4.10. — 如果 $a,b\in\mathbf{Z}_p$, 且 $|a-b|_p\leqslant p^{-1}$, 则 $|a^p-b^p|_p\leqslant p^{-1}|a-b|_p$.

[491] 证明 $a^p-b^p=p(a-b)\sum_{i=0}^{p-1}\frac{1}{p}\binom{p}{i}(a-b)^{p-i-1}$, 而由假设 $|a-b|_p\leqslant p^{-1}$ 以及当 $1\leqslant i\leqslant p-1$ 时 $\binom{p}{i}$ 被 p 整除的事实 (小词典的习题 1.4) 得知, 和号中的每一项都属于 $\mathbf{Z}_p$. 由此得到结论. □

命题 D.4.11. — (i) 如果 $a\in\mathbf{Z}_p$, 则序列 $(a^{p^n})_{n\in\mathbf{N}}$ 有一个满足 $|a-\omega(a)|_p\leqslant p^{-1}$ 的极限 $\omega(a)\in\mathbf{Z}_p$.

(ii) 如果 $a\in p\mathbf{Z}_p$, 则 $\omega(a)=0$, 如果 $a\in\mathbf{Z}_p^*$, 则 $\omega(a)\in\boldsymbol{\mu}_{p-1}$.

(iii) 对于每对 $a,b\in\mathbf{Z}_p$ 有 $\omega(ab)=\omega(a)\omega(b)$.

证明 如果 $a\in\mathbf{N}$, 根据费马小定理知 $|a^p-a|_p\leqslant p^{-1}$. 由于 $\mathbf{N}$ 在 $\mathbf{Z}_p$ 中稠密, 这个不等式由 $a\mapsto|a^p-a|_p$ 的连续性知对于 $a\in\mathbf{Z}_p$ 也为真. 引理 D.4.10 让我们可以通过对 n 的归纳由此得到 $|u_{n+1}-u_n|_p\leqslant p^{-n}$, 在这里的 $u_n=a^{p^n}$. 因为 $u_{n+1}-u_n\to 0$, 故得知 u_n 有一个极限 $\omega(a)$, 并且 $a-\omega(a)=\sum_{n=0}^{+\infty}(u_n-u_{n+1})$ 的范数 $\leqslant\sup_{n\in\mathbf{N}}|u_n-u_{n+1}|_p\leqslant p^{-1}$. 由此得 (i).

现在, 因为 $\omega(a)^p$ 是序列 $(a^{p^{n+1}})_{n\in\mathbf{N}}$ 的极限, 故 $\omega(a)^p=\omega(a)$.

- 如果 $a\in p\mathbf{Z}_p$, 则 $|a^{p^n}|_p\leqslant p^{-p^n}$, 从而 $a^{p^n}\to 0$, 于是 $\omega(a)=0$.
- 如果 $a\in\mathbf{Z}_p^*$, 则由于 $|a|_p=1$ 和 $|a-\omega(a)|_p\leqslant p^{-1}$, 故 $\omega(a)\neq 0$. 因为 $\omega(a)^p=\omega(a)$, 故有 $\omega(a)^{p-1}=1$, 这证明了 (ii).

最后, $\omega(ab)=\lim(ab)^{p^n}=\lim a^{p^n}b^{p^n}=\omega(a)\omega(b)$. □

注记 D.4.12. — (i) 从上一个命题得知 $\omega:\mathbf{Z}_p^*\to\boldsymbol{\mu}_{p-1}$ 是一个线性特征标; 称其为泰希米勒 (Teichmüller) 特征标.

(ii) 如果 $x\in\mathbf{Z}_p^*$, 令 $\langle x\rangle=\omega(x)^{-1}x$. 因为 $|x-\omega(x)|_p\leqslant p^{-1}$, 故有 $|\langle x\rangle-1|_p\leqslant p^{-1}$.

命题 D.4.13. — (i) 如果 $s\in\mathbf{Z}_p$, 且 $i\in\mathbf{Z}/(p-1)\mathbf{Z}$, 则对于 $n\in\mathbf{N}, n\equiv i \bmod p-1$

的通项为 x^n 的序列有极限 (记其为 $x^{s,i}$).

(ii) 如果 $x \in p\mathbf{Z}_p$, 则 $x^{s,i}=0$, 而如果 $x \in \mathbf{Z}_p^*$, 则 $x^{s,i}=\omega(x)^i\langle x\rangle^s$.

(iii) 如果 $n \in \mathbf{Z}$ 且与 $i \bmod p-1$ 同余, 而 $x \in \mathbf{Z}_p^*$, 则 $x^{n,i}=x^n$.

证明 • 如果 $x \in 1+p\mathbf{Z}^p$, 如我们已经知道的, 函数 $s \mapsto x^s=\sum_{n=0}^{+\infty}\binom{s}{n}(x-1)^n$ 是连续的, 并当 $s=n$ 时取值 x^n. 由此得到 $x^{s,i}=x^s$ 的存在性.

• 如果 $x \in p\mathbf{Z}_p$, 通项为 x^n 的序列当 n 趋向 $+\infty$ 时趋向 0.

• 如果 $x \in \mathbf{Z}_p^*$, 则可将 x 写成 $\omega(x)\langle x\rangle$ 的形式, 从而 x^n 写为 $\omega(x)^n\langle x\rangle^n$.

由于 $\langle x\rangle \in 1+p\mathbf{Z}_p$, 函数 $n \mapsto \langle x\rangle^n$ 可连续地扩张, 而 $\omega(x)$ 作为一个 $p-1$ 次单位根, 函数 $n \mapsto \omega(x)^n$ 是周期为 $p-1$ 的周期函数. 这使得, 如果固定一个 $i \in \{0,1,\ldots,p-1\}$, 且 $x \in \mathbf{Z}_p^*$, 从 $i+(p-1)\mathbf{N}$ 到 $\mathbf{Z}_p$ 的函数 $x \mapsto x^n$ 可以连续地扩张为 $\mathbf{Z}_p$ 上的一个连续函数.

由此推导出了 (i) 和 (ii). (iii) 则来自, 如果 $n \in \mathbf{Z}$, 则 $\langle x\rangle^n = x^n\omega(x)^n$, 而如果 $n \equiv i \bmod p-1$ 且 $x \in \mathbf{Z}_p^*$, 则 $\omega(x)^n=\omega(x)^i$. □

引理 D.4.14. — 如果 μ 是 $\mathbf{Z}_p$ 上的一个测度, 且若 $i \in \mathbf{Z}/(p-1)\mathbf{Z}$, 则 $s \mapsto \int_{\mathbf{Z}_p} x^{s,i}\mu$ 在 $\mathbf{Z}_p$ 上连续.

证明 我们有 $x^{s,t}=\sum_{n=0}^{+\infty}\binom{s}{n}\Big(\mathbf{1}_{\mathbf{Z}_p^*}(x)\omega(x)^i(\langle x\rangle-1)^n\Big)$, 且由于当 $s \in \mathbf{Z}_p$ 时有 $|\binom{s}{n}|_p \leqslant 1$ 以及 $\|\mathbf{1}_{\mathbf{Z}_p^*}(x)\omega(x)^i(\langle x\rangle-1)^n\|_\infty \leqslant p^{-n}$, 故这个级数在 $\mathscr{C}(\mathbf{Z}_p)$ 中收敛, 这让我们可以交换级数和积分, 从而得到 $\int_{\mathbf{Z}_p} x^{s,i}\mu=\sum_{n=0}^{+\infty}a_n\binom{s}{n}$, 其中 $a_n=\int_{\mathbf{Z}_p}\mathbf{1}_{\mathbf{Z}_p^*}(x)\omega(x)^i(\langle x\rangle-1)^n\mu$. 因此我们有 $|a_n|_p \leqslant p^{-n}\|\mu\|_\infty$, 于是 $a_n \to 0$. 得到了结论.(控制函数 $|a_n|_p \leqslant p^{-n}\|\mu\|_\infty$ 实际上证明了当 $p \geqslant 3$ 时, $s \mapsto \int_{\mathbf{Z}_p} x^{s,i}\mu$ 是解析的 (如果 $p=2$, 这个函数在 $2\mathbf{Z}_2$ 和在 $1+2\mathbf{Z}_2$ 上解析).) □ [492]

4. μ_a 在 $\mathbf{Z}_p^*$ 上的限制

如果 U 是 $\mathbf{Z}_p$ 的一个开紧集, 且 μ 是 $\mathbf{Z}_p$ 上的一个测度, 那么我们以 $\mathrm{Res}_U\mu$ 表示 μ 在 U 上的限制: 这是一个由 $\int_{\mathbf{Z}_p}\phi\mathrm{Res}_U\mu=\int_{\mathbf{Z}_p}\mathbf{1}_U\phi\mu$ 定义的测度 (我们也将其记为 $\int_U\phi\mu$). 后面的推论 D.4.18[3]证明了将 μ_a 限制到 $\mathbf{Z}_p^*$ 分离出一个含 p 的欧拉因子. 很不寻常的是, 一个测度和它在 $\mathbf{Z}_p^*$ 的限制之间的关联也是简单的.

引理 D.4.15. — 设 c 是一个 $\geqslant 1$ 的整数, 且 $i \in \{0,1,\ldots,c-1\}$.

(i) $\lim_{z\to 0}\frac{(1+z)^i}{(1+z)^c-1}-\frac{1}{cz}=\frac{i}{c}-\frac{c-1}{2c}$.

(ii) $\frac{1}{c}\sum_{\eta\in\boldsymbol{\mu}_c-\{1\}}\frac{\eta^{-i}}{\eta-1}=\frac{i}{c}-\frac{c-1}{2c}$.

(iii) 如果 $(a,c)=1$, 则 $\frac{1}{c}\sum_{\eta\in\boldsymbol{\mu}_c-\{1\}}\frac{\eta^{-i}}{\eta^c-1}=\frac{[a^{-1}i]}{c}-\frac{c-1}{2c}$, 其中 $[a^{-1}i] \in \{0,1,\ldots,c-1\}$ 是 $a^{-1}i \in \mathbf{Z}/c\mathbf{Z}$ 的代表元.

[3]所提出的这个证明相当笨拙但它让我们不会离开 $\mathbf{Q}_p$; 习题 D.4.19 提出了一个更优雅的证明.

证明 我们有 $\frac{(1+z)^i}{(1+z)^c-1}=\frac{1+iz+\cdots}{cz(1+\frac{c-1}{2}z+\cdots)}=\frac{1}{cz}(1+iz-\frac{c-1}{2}z+\cdots)$, 由此得 (i).

我们有 $\frac{1}{c}\sum_{\eta\in\boldsymbol{\mu}_c-\{1\}}\frac{\eta^i}{\eta-1}=\lim_{z\to 0}\frac{1}{c}\sum_{\eta\in\boldsymbol{\mu}_c}\frac{\eta^{-i}}{(1+z)\eta-1}-\frac{1}{cz}$ 和 $\frac{1}{c}\sum_{\eta\in\boldsymbol{\mu}_c}\frac{\eta^{-i}}{(1+z)\eta-1}=\frac{(1+z)^i}{(1+z)^c-1}$(如果 $\eta\in\boldsymbol{\mu}_c$, 它由 $\lim_{z\to\eta^{-1}-1}((1+z)\eta-1)\frac{(1+z)^i}{(1+z)^c-1}=\frac{\eta^{-i}\eta}{c(\eta^{-1})^{c-1}}=\eta^{-i}$ 得到). 因此 (ii) 是 (i) 的推论.

最后, 因为 $(a,c)=1$, 于是 $\eta\mapsto\eta^a$ 是 $\boldsymbol{\mu}_c$ 间的双射, 而且如果 $\eta\in\boldsymbol{\mu}_c$ 有 $\eta^{-i}=(\eta^a)^{-[a^{-1}i]}$, 这让我们从 (ii) 推出 (iii). □

如果 $b\in\mathbf{Q}_p$ 按 p 的记数法为 $\sum_{i=-k}^{+\infty}p^ib_i$(这些 b_i 属于 $\{0,\ldots,p-1\}$). 并以 $\{b\}$ 记 $\mathbf{Q}$ 的元 $\sum_{i=-k}^{-1}p^ib_i$: 它是 $\mathbf{Z}[\frac{1}{p}]\cap[0,1[$ 中使得 $b-\{b\}\in\mathbf{Z}_p$ 的唯一的元. 我们有: $\{b\}=\{b'\}$ 当且仅当 $b-b'\in\mathbf{Z}_p$.

引理 D.4.16. — 对于所有的 $i\in\mathbf{Z}_p$ 和 $n\in\mathbf{N}$ 有 $\mu_a(i+p^n\mathbf{Z}_p)=\{\frac{i}{p^n}\}-a\{\frac{a^{-1}i}{p^n}\}+\frac{a-1}{2}$.

证明 如有必要可将 i 换成它的 mod p^n 的代表元, 于是可以假设 $i\in\{0,1,\ldots,p^n-1\}$. 根据推论 D.4.6, 有

$$\begin{aligned}\mu_a(i+p^n\mathbf{Z}_p)&=\frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}}\eta^{-i}\mathscr{A}_{\mu_a}(\eta-1)\\&=\frac{1}{p^n}\mathscr{A}_{\mu_a}(0)+\frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}-\{1\}}(\frac{\eta^{-i}}{\eta-1}-a\frac{\eta^{-i}}{\eta^a-1}).\end{aligned}$$

[493] 从引理 D.4.15 的 (i) 得到 $\mathscr{A}_{\mu_a}(0)=\frac{1-a}{2}$, 而从同一引理的 (ii) 和 (iii) 得到

$$\frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}-\{1\}}\frac{\eta^{-i}}{\eta-1}=\frac{i}{p^n}-\frac{p^n-1}{2p^n}$$

和

$$\frac{1}{p^n}\sum_{\eta\in\boldsymbol{\mu}_{p^n}-\{1\}}\frac{\eta^{-i}}{\eta^a-1}=\frac{[a^{-1}i]}{p^n}-\frac{p^n-1}{2p^n}.$$

注意到有 $\{\frac{a^{-1}i}{p^n}\}=\frac{[a^{-1}i]}{p^n}$ 便得到结果. □

引理 D.4.17. — 对于 $\phi\in\mathscr{C}(\mathbf{Z}_p)$, 我们有 $\int_{p\mathbf{Z}_p}\phi(\frac{x}{p})\mu_a=\int_{\mathbf{Z}_p}\phi\mu_a$.

证明 如果 $\phi\in\mathscr{C}(\mathbf{Z}_p)$, 定义函数 $[p]\cdot\phi$ 为: 当 $x\in p\mathbf{Z}_p$ 时 $([p]\cdot\phi)(x)=\phi(\frac{x}{p})$, 而当 $x\in\mathbf{Z}_p^*$ 时 $([p]\cdot\phi)(x)=0$. 于是 $[p]\cdot\phi\in\mathscr{C}(\mathbf{Z}_p)$, 且 $[p]:\mathscr{C}(\mathbf{Z}_p)\to\mathscr{C}(\mathbf{Z}_p)$ 是线性的, 并且因为 $\|[p]\cdot\phi\|_\infty\leqslant\|\phi\}_\infty$, 知其连续. 从而 $\lambda=\mu_a\circ([p]-1)$ 是 $\mathbf{Z}_p$ 上的一个测度. 现在, 如果 $i\in\mathbf{Z}_p$ 和 $n\in\mathbf{N}$, 则因为 $\frac{x}{p}\in i+p^n\mathbf{Z}_p$ 等价于 $x\in pi+p^{n+1}\mathbf{Z}_p$, 故 $[p]\cdot\mathbf{1}_{i+p^n\mathbf{Z}_p}=\mathbf{1}_{pi+p^{n+1}\mathbf{Z}_p}$. 因此按照引理 D.4.16 有

$$\begin{aligned}\int_{\mathbf{Z}_p}\mathbf{1}_{i+p^n\mathbf{Z}_p}\lambda&=\mu_a(i+p^n\mathbf{Z}_p)-\mu_a(pi+p^{n+1}\mathbf{Z}_p)\\&=(\{\frac{i}{p^n}\}-a\{\frac{a^{-1}i}{p^n}\}+\frac{a-1}{2})-(\{\frac{pi}{p^{n+1}}\}-a\{\frac{a^{-1}pi}{p^{n+1}}\}+\frac{a-1}{2})=0.\end{aligned}$$

由线性性推出 λ 在 $\mathrm{LC}(\mathbf{Z}_p)$ 上恒等于 0, 并因为 $\mathrm{LC}(\mathbf{Z}_p)$ 在 $\mathscr{C}(\mathbf{Z}_p)$ 中稠密, 故 λ 也在 $\mathscr{C}(\mathbf{Z}_p)$ 上恒为 0, 另外也得到 λ 是连续的. 由此, 并因为 $\int_{\mathbf{Z}_p}\phi\lambda = \int_{p\mathbf{Z}_p}\phi(\frac{x}{p})\mu_a - \int_{\mathbf{Z}_p}\phi\mu_a$, 便得到了结果. □

推论 D.4.18. — 如果 $n\in\mathbf{N}$, 则 $\int_{\mathbf{Z}_p^*}x^n\mu_a = (-1)^n(1-a^{n+1})(1-p^n)\zeta(-n)$.

证明　根据引理 D.4.17 有 $\int_{\mathbf{Z}_p^*}x^n\mu_a = \int_{\mathbf{Z}_p}x^n\mu_a - \int_{p\mathbf{Z}_p}x^n\mu_a$ 以及

$$\int_{p\mathbf{Z}_p}x^n\mu_a = p^n\int_{p\mathbf{Z}_p}(\frac{x}{p})^n\mu_a = p^n\int_{\mathbf{Z}_p}x^n\mu_a.$$

那么由命题 D.4.8 得到结论. □

习题 D.4.19. — (i) 建立公式 $\mathbf{1}_{\mathbf{Z}_p^*}(x) = 1 - \frac{1}{p}\sum_{\eta\in\boldsymbol{\mu}_p}\eta^x$.

(ii) 由此推出, 如果 μ 是 $\mathbf{Z}_p$ 上的一个测度, 则 $\mathrm{Res}_{\mathbf{Z}_p^*}\mu$ 的阿米斯变换为 $\mathscr{A}_\mu(T) - \frac{1}{p}\sum_{\eta\in\boldsymbol{\mu}_P}((1+T)\eta-1)$.

(iii) 证明 $\mathrm{Res}_{\mathbf{Z}_p^*}\mu_a$ 的阿米斯变换是 $\mathscr{A}_{\mu_a} - \mathscr{A}_{\mu_a}((1+T)^p-1)$, 并由此重新证明推论 D.4.18 的结果.

D.5. 构造 p-adic ζ 函数

转向定理 D.4.1 的证明. 如果 $i\in\mathbf{Z}/(p-1)\mathbf{Z}$, 而 $a\in\mathbf{Z}_p^*$, 定义 $\mathbf{Z}_p$ 上的函数 $g_{a,i}$ 为

$$g_{a,i} = \frac{1}{1-\omega(a)^{1-i}\langle a\rangle^{1-s}}\int_{\mathbf{Z}_p^*}\omega(x)^{-i}\langle x\rangle^{-s}\mu_a(x).$$

根据引理 D.4.14, 这个函数在函数 $s\mapsto 1-\omega(a)^{1-i}\langle a\rangle^{1-s}$ 的零点外连续. 另外, 如果 $-n\equiv i \bmod [p-1]$, 则有 $\omega(a)^{1-i} = \omega^{1+n}$, 而又如果 $x\in\mathbf{Z}_p^*$, 则 $\omega(x)^{-i} = \omega(x)^n$, 因此, 根据推论 D.4.18 有 [494]

$$\begin{aligned} g_{a.i}(-n) &= \frac{1}{1-\omega(a)^{1+n}\langle a\rangle^{1+n}}\int_{\mathbf{Z}_p^*}\omega(x)^n\langle x\rangle^n\mu_a(x) \\ &= \frac{1}{1-a^{1+n}}\int_{\mathbf{Z}_p^*}x^n\mu_a(x) \\ &= (-1)^n(1-p^n)\zeta(-n). \end{aligned}$$

为了得到结论, 故而只需找到一个 a, 它使得函数 $s\mapsto 1-\omega(a)^{1-i}\langle a\rangle^{1-s}$ 当 $i\neq 1$ 时不为零, 而只当 $i=1$ 时的 $s=1$ 为零.

- $1-\omega(a)^{1-i}\langle a\rangle^{1-s}$ 在 $\mathbf{F}_p$ 中的像是 $1-a^{1-i}$ 在 $\mathbf{F}_p$ 中的像. 现在, 如果 $i\neq 1$, 则可选取 i 在 $\mathbf{Z}$ 中属于 $\{2,\ldots,p-1\}$ 的代表元, 它使得方程 $x^{1-i}=1$ 当 $i\neq 1$ 时在 $\mathbf{F}_p$ 中有少于 $p-2$ 个解. 因此存在 $a\in\mathbf{N}$ 使得 $1-a^{1-i}$ 在 $\mathbf{F}_p$ 中非零, 并且对这样的一个 a, 函数 $s\mapsto 1-\omega(a)^{1-i}\langle a\rangle^{1-s}$ 不取零.

如果 $u \in 1+p\mathbf{Z}_p$, 且 $x \in \mathbf{Z}_p - \{0\}$ 满足 $u^x = 1$, 于是对于每个 $a \in \mathbf{N}$ 有 $u^{ax} = 1$. 由于 $\mathbf{N}$ 在 $\mathbf{Z}_p$ 中稠密和 $a \mapsto u^{ax}$ 的连续性, 因此这个等式对于所有的 $a \in \mathbf{Z}_p$ 都成立. 如果 $v_p(x) = k$, 而 $a = p^k x^{-1}$, 则有 $a \in \mathbf{Z}_p$, 从而 $u^{p^k} = 1$. 这证明了函数 $u \mapsto u^x - 1$ 在 u 不是 p 的幂次阶的单位根时便不为零. 这样, 我们便可在 $\mathbf{N}$ 中取 a 为使 $\langle a \rangle$ 不是单位根的元 (例如 $a = 1 + 2p$), 因此 $s \mapsto 1 - \omega(a)^{1-i}\langle a \rangle^{1-s}$ 当 $i = 0$ 时只在 $s = 1$ 取零.

附录 E. 无穷个无理数的 $\zeta(2n+1)$

本附录致力于讲解 Rivoal 的结果 (2000), 我们在第 III 章的脚注 9 提到过它; 按此结果, 存在无穷多个 $n \geqslant 1$ 使得 $\zeta(2n+1)$ 是无理数. 我们实际上将证明一个更强的结果 (参看下面的定理 E.1.1 的 (i)).

E.1. 实数的线性无关性

如果对 $i \in I$, v_i 是一些实数, 则以 $\mathrm{Vect}(v_i, i \in I)$ 记 $\mathbf{R}$ 中由这些 v_i 生成的 $\mathbf{Q}$-向量子空间, 并以 $\dim_{\mathbf{Q}} \mathrm{Vect}(v_i, i \in I)$ 记其维数. 例如, v 是无理数当且仅当 $\dim_{\mathbf{Q}}(1, v) = 2$.

定理 E.1.1. — (i) $\dim_{\mathbf{Q}} \mathrm{Vect}(\zeta(2n+1), n \geqslant 1) = +\infty$.

(ii) $\dim_{\mathbf{Q}} \mathrm{Vect}(\zeta(2n), n \geqslant 1) = +\infty$.

注记 E.1.2. — (i) 定理的 (ii) 可以让我们重新证明 Lindemann (1882) 证过的 π 的超越性. 事实上, 由于 $\zeta(2n) \in \mathbf{Q}\pi^{2n}$(参看习题 V.5.3), 那么 (ii) 等价于以下断言中的任一个:

- $\dim_{\mathbf{Q}} \mathrm{Vect}(\pi^{2n}, n \geqslant 1) = +\infty$.
- π 是超越数.
- 1 和 $\pi^{2n}, n \geqslant 1$ 在 $\mathbf{Q}$ 上线性无关.
- 1 和 $\zeta(2n), n \geqslant 1$ 在 $\mathbf{Q}$ 上线性无关.

(ii) 人们猜测, 1 和那些 $\zeta(n), n \geqslant 2$ 在 $\mathbf{Q}$ 上线性无关, 但离知此断言的证明尚远: 特别地, 还不知如何证明 $\zeta(5)$ 是无理的; $\zeta(3)$ 的无理性 (问题 H.12) 证明则要追溯到 1979 年 (Apéry).

1. Nesterenko 判别法

为了证明两个数 v_1, v_2 在 $\mathbf{Q}$ 上线性无关, 只需造出两个整数的序列 $(a_{n,i})_{n\in\mathbf{N}}, i=1,2$, 使得对于充分大的 n 有 $a_{n,1}v_1+a_{n,2}v_2\neq 0$, 而 $\lim_{n\to+\infty} a_{n,1}v_1+a_{n,2}v_2=0$ 就可以了 (事实上, 如果 $v_2=\frac{c}{d}v_1$, 其中 $d\in\mathbf{N}-\{0\}, c\in\mathbf{Z}$, 那么, 如果 $a_1,a_2\in\mathbf{Z}$ 以及 $a_1v_1+a_2v_2\neq 0$, 则有 $|a_1v_1+a_2v_2|=|\frac{da_1+ca_2}{d}||v_1|\geqslant\frac{1}{d}|v_1|$). 在一般情形, 我们给出下面属于 Nesterenko 的判别法.

[496] **定理 E.1.3.** — (Nesterenko 判别法) 设 $v_1,\ldots,v_b\in\mathbf{R}$. 假设存在 $A>1, B>1$ 以及对每个 $n\in\mathbf{N}$ 的具有整系数的线性组合 $L_n=a_{n,1}v_1+\cdots+a_{n,b}v_b$, 满足

(i) $\sum_{1\leqslant j\leqslant b}|a_{n,j}|\leqslant B^{n+o(n)}$;

(ii) $|a_{n,1}v_1+\cdots+a_{n,b}v_b|=A^{-n+o(n)}$.

于是 $\dim_{\mathbf{Q}}\mathrm{Vect}(v_1,\ldots,v_b)\geqslant 1+\frac{\log A}{\log B}$.

在我们所感兴趣的情形中, 我们从在 $\leqslant 0$ 的整数上只具有极点的有理函数着手, 给出了构建在那些 $\zeta(n), n\geqslant 2$ 之间具有理系数的线性关系的一个机制 (参看命题 E. 2.1), 因此, 问题在于必须选好这些有理函数, 以使得如此得到的线性组合能够用得上 Nesterenko 判别法.

证明 不妨对 $v_1,\ldots,v_b$ 除以 v_1, 从而可假定 $v_1=1$. 设 $1=w_0,w_1,\ldots,w_r$ 是 $\mathrm{Vect}(v_1,\ldots,v_b)$ 在 $\mathbf{Q}$ 上的一组基. 可以将这些 v_i 用这组基来表示, 并对此表示乘以这些 v_i 坐标的分母的最小公倍数; 于是这些 L_n 成为 $w_0,\ldots,w_r$ 的整数系数的线性组合并满足与定理陈述中同样的估值 (其中新的 $o(n)$ 与原来的 $o(n)$ 差一个加法常数项). 因此问题化为证明以下的断言:

如果 $1=w_0,\ldots,w_r$ 在 $\mathbf{Q}$ 上线性无关, 且存在 $B>1, A>1$ 和具有整系数的线性形式 $L_n(x_0,\ldots,x_r)=a_{n,0}x_0+\cdots+a_{n,r}x_r$, 使得 $\sum_{j=0}^r|a_{n,j}|\leqslant B^{n+o(n)}$ 和 $\Lambda_n=|L_n(w_0,\ldots,w_r)|^{-1}=A^{n+o(n)}$, 则 $\frac{\log A}{\log B}\leqslant r$.

令 $C_n=\{(x_0,\ldots,x_r)\in\mathbf{R}^{r+1}, |x_0|\leqslant\Lambda_n$ 以及当 $1\leqslant i\leqslant r$ 时 $|x_0w_i-w_0|\leqslant\Lambda_n^{-1/r}\}$. 于是 C_n 是 $\mathbf{R}^{r+1}$ 中的一个平行多面体, 其体积为 $(2\Lambda_n)\prod_{i=1}^r(2\Lambda_n^{-1/r})=2^{r+1}$. 由此知 C_n 是一个体积为 2^{r+1} 的对称的凸紧集, 而闵可夫斯基引理 (定理 B. 1.12) 确保了有一个属于 $C_n-\{0\}$ 的 $(x_0(n),\ldots,x_r(n))\in\mathbf{Z}^{r+1}$ 的存在性.

如果 $n\gg 0$, 令 $k(n)$ 为使得 $|x_0(n)|\Lambda_{k(n)}^{-1}\leqslant\frac{1}{2}$ 的最大整数. $\Lambda_n=A^{n+o(n)}$ 这个假设条件表明 $k(n)=\frac{\log|x_0(n)|}{\log A}+o((\log|x_0(n)|)$, 因此

- $k(n)\leqslant\frac{\log\Lambda_n}{\log A}+o(\log\Lambda_n)=n+o(n)$,
- $\Lambda_{k(n)}=|x_0(n)|^{1+o(1)}$ 以及 $|x_0(n)L_{k(n)}(w_0,\ldots,w_r)|=|x_0(n)|^{o(1)}=\Lambda_n^{o(1)}=A^{o(1)}$.

现在,$\sum_{i=0}^r a_{k(n),i}x_i(n)=x_0(n)L_{k(n)}(w_0,\ldots,w_r)+\sum_{i=0}^r a_{k(n),i}(x_i(n)-x_0(n)w_i)$. 但是其左端是一个整数, 而由构造知 $|x_0(n)L_{k(n)}(w_0,\ldots,w_r)|\leqslant\frac{1}{2}$. 于是

$$|\sum_{i=0}^{r} a_{k(n),i}(x_i(n) - x_0(n)w_i)| \geqslant |x_0(n)L_{k(n)}(w_0,\ldots,w_r)| = A^{o(n)}.$$

左端被强函数 $(\sum_{i=0}^{r}|a_{k(n),i}|)\Lambda_n^{-1} \leqslant B^{k(n)+o(k(n))}A^{-n/r+o(n)}$ 控制, 并由于 $k(n) \leqslant n+o(n)$, 故有 $B^{k(n)+o(k(n))} \leqslant B^{n+o(n)}$. 因此得到 $B^{n+o(n)}A^{-n/r+o(n)} \geqslant A^{o(n)}$, 它给出了 $BA^{-1/r} \geqslant 1$ 和 $r \geqslant \frac{\log A}{\log B}$, 即为所要证明的[1]. □

E.2. π 的超越性和 $\zeta(n)$ 的线性无关性 [497]

1. 生成 $\zeta(n)$ 间的线性组合

设 $a \in \mathbf{N}$ 且 $F \in \mathbf{Q}(X)$ 是 $\leqslant -2$ 次并只在 $\leqslant 0$ 的整数上有极点, 且这些极点的阶是 $\leqslant a$ 的有理函数. 设 $\alpha_{j,k}, j \geqslant 0, 1 \leqslant k \leqslant a$ 和 $\alpha_k, 1 \leqslant k \leqslant a$ 被有理函数 $F(X)$ 的简单分式分解定义:

$$F(X) = \sum_{j=0}^{+\infty}\sum_{k=1}^{a}\frac{\alpha_{j,k}}{(X+j)^k} \text{ 及 } \alpha_k = \sum_{j=0}^{+\infty}\alpha_{j,k}.$$

我们注意, 除了有限个偶对 (j,k) 外 $\alpha_{j,k}=0$, 从而上面的这个级数事实上是个有限和, 另一方面, 因为我们假设了 F 的次数 $\leqslant -2$, 故 $\alpha_1 = 0$.

命题 E.2.1. — 级数 $\sum_{m=1}^{+\infty}F(m)$ 绝对收敛, 并有

$$\sum_{m=1}^{+\infty}F(m) = \sum_{k=2}^{a}\alpha_k\zeta(k) - \sum_{k=1}^{a}\sum_{j=0}^{+\infty}\alpha_{j,k}\left(\sum_{u=1}^{j}\frac{1}{u^k}\right).$$

证明 这个绝对收敛性来自假设条件 $\deg F \leqslant -2$. 如果 $N \in \mathbf{N}$ 是使得当 $j \geqslant N+1$ 时有 $\alpha_{j,k}=0$ 的数, 于是有

$$\sum_{m=1}^{M}\sum_{j=0}^{N}\frac{\alpha_{j,1}}{m+j} = \left(\sum_{j=0}^{N}\alpha_{j,1}\right)\left(\sum_{u=1}^{N+M}\frac{1}{u}\right) - \sum_{j=0}^{N}\alpha_{j,1}\left(\sum_{u=1}^{j}\frac{1}{u} + \sum_{u=M+j+1}^{N+M}\frac{1}{u}\right),$$

而因为 $\sum_{j=0}^{N}\alpha_{j,1}=0$, 在将 M 趋向 $+\infty$ 时便得到

$$\sum_{m=1}^{+\infty}\sum_{j=0}^{N}\frac{\alpha_{j,1}}{m+j} = -\sum_{j=0}^{N}\alpha_{j,1}\left(\sum_{u=1}^{j}\frac{1}{u}\right).$$

另一方面, 我们有

$$\sum_{m=1}^{+\infty}\sum_{j=0}^{N}\sum_{k=2}^{a}\frac{\alpha_{j,k}}{(m+j)^k} = \sum_{k=2}^{a}\sum_{j=0}^{N}\sum_{u=j+1}^{+\infty}\frac{\alpha_{j,k}}{u^k} = \sum_{k=2}^{a}\sum_{j=0}^{N}\alpha_{j,k}\left(\zeta(k) - \sum_{u=1}^{j}\frac{1}{u^k}\right)$$
$$= \sum_{k=2}^{a}\alpha_k\zeta(k) - \sum_{k=2}^{a}\sum_{j=0}^{N}\alpha_{j,k}\left(\sum_{u=1}^{j}\frac{1}{u^k}\right),$$

[1] 这个证明属于 Fischler 和 Zudilin(2010); 它比 Nesterenko 原来的证明要简单得多.

为得到结论只要将上面的两个表达式求和即可. □

2. 明智地选取有理函数

设 $a, r \in \mathbf{N}$ 满足 $2r \leqslant a$ 且 $r \geqslant 1$. (我们要寻找在 1 和 $\zeta(k), k \leqslant a$ 之间的整系数
[498] 的线性组合, 而 r 是一个用来调节的参数以使这些线性组合尽可能地小). 设

$$F_n(X) = (n!)^{a-2r}\frac{(X-rn)(X-rn+1)\cdots(X+(r+1)n)}{(X(X+1)\cdots(X+n))^{a+1}}$$
$$= (n!)^{a-2r}\frac{(X-rn)\cdots(X-1)(X+n+1)\cdots(X+(r+1)n)}{(X(X+1)\cdots(X+n))^{a}}.$$

$\alpha_{j,k}^{(n)}, 0 \leqslant j \leqslant n, 1 \leqslant k \leqslant \alpha$, 且 $\alpha_k^{(n)}, 1 \leqslant k \leqslant a$ 是通过 $F_n(X)$ 的简单分式分解由

$$F_n(X) = \sum_{j=0}^{n}\sum_{k=1}^{a}\frac{\alpha_{j,k}^{n}}{(X+j)^k} \text{ 和 } \alpha_k^{(n)} = \sum_{j=0}^{n}\alpha_{j,k}^{(n)}$$

定义的.

这个有理分式有几个有趣的性质.

- F_n 的次数 $(2r+1)n+1-(n+1)(a+1) = (2r-a)n-a \leqslant -a \leqslant -2$, 且在 $0, -1, \ldots, -n$ 具有 a 阶极点; 级数 $S_n = \sum_{m=1}^{+\infty} F_n(m)$ 收敛从而绝对收敛, 并有

$$S_n = \beta^{(n)} + \sum_{k=2}^{a}\alpha_k^{(n)}\zeta(k),$$

其中 $\beta^n = -\sum_{k=1}^{a}\sum_{j=0}^{n}\alpha_{j,k}^{(n)}(\sum_{u=1}^{j}\frac{1}{u^k})$.

- $F_n(1) = \cdots = F_n(rn) = 0$, 这证明了定义 S_n 的那个和仅从 $m = rn+1$ 开始 (即 $S_n = \sum_{m=0}^{+\infty} F_n(rn+m+1)$, 这确保了 S_n 是小的.
- 当 $m \geqslant 1$ 时 $F_n(m) \geqslant 0$, 这确保了 S_n 非零.
- F_n 满足函数方程 $F_n(-n-X) = (-1)^{(n+1)a}F_n(X)$, 如果 $1 \leqslant k \leqslant a$ 和 $0 \leqslant j \leqslant n$, 则此方程给出了关系式 $\alpha_{n-j,k}^{(n)} = (-1)^{k+(n+1)a}\alpha_{j,k}^{(n)}$; 这些关系式表明当 $k+(n+1)a$ 为奇数时 $\alpha_k^{(n)} = 0$, 这是将在偶整数上的值从在奇整数上的值分割开来的关键之处. (为了只观察在偶数上的值, 只需取 a 为偶数即可, 而为了观察在奇数上的值则只要取 a 为奇数而 n 为偶数即可.)

为了能应用 Nestrenko 判别法 (参看 5 小节), 这关系到 S_n 的精确取值 (参看 4 小节), 涉及给出对系数 $\alpha_k^{(n)}$ 的强函数, 并因为需要线性组合是整数系数的, 还涉及它们的分母的最小公倍数 (参看 3 小节).

3. $\alpha_k^{(n)}$ 的阿基米德性质和算术性质

以 d_n 代表 $1, 2, \ldots, n$ 的最小公倍数.

命题 E.2.2. — 如果 $1 \leqslant k \leqslant a$ 和 $0 \leqslant j \leqslant n$, 则

$$d_n^{a-k}\alpha_{k,j}^{(n)} \in \mathbf{Z} \text{ 以及 } |\alpha_{k,j}^{(n)}| \leqslant (2n)^{a-1}(a-1)!2^{na}(r+1)^{2(r+1)n}.$$

推论 E.2.3. — (i) 如果 $n \in \mathbf{N}$ 且 $k \in \{2, \ldots, a\}$, 则 $d_n^a\beta^{(n)} \in \mathbf{Z}$ 且 $d_n^{a-k}\alpha_k^{(n)} \in \mathbf{Z}$.

(ii) 如果 $\delta > 2^a(r+1)^{2r+2}$, 则 $|\beta^{(n)}| = O(\delta^n)$ 并且对所有的 $k \in \{2, \ldots, a\}$ 有 $|\alpha_k^{(n)}| = O(\delta^n)$.

证明 (i) $d_n^{a-k}\alpha_k^{(n)} = \sum_{j=0}^n d_n^{a-k}\alpha_{k,j}^{(n)}$, 故立即知其属于 $\mathbf{Z}$; 而 $d_n^a\beta^{(n)} = -\sum_{k=1}^a(\sum_{j=0}^n d_n^{a-k}\alpha_{k,j}^{(n)}(\sum_{u=1}^j \frac{d_n^k}{u^k}))$ 属于 $\mathbf{Z}$ 由下面事实得到: 因为 $u \leqslant j \leqslant n$ 蕴含了 $u \mid d_n$, 故上式右端的每项都是整数. [499]

(ii) 这个命题表明, 当 $\delta > 2^a(r+1)^{2r+2}$ 时有 $|\alpha_k^{(n)}| \leqslant (n+1)(2n)^{a-1}(a-1)!2^{na}(r+1)^{2(r+1)n} = O(\delta^n)$. 另外, 我们还有囿于上的函数关系 $\sum_{u=1}^j \frac{1}{u^k} \leqslant j \leqslant n$, 因而对于所有的 $\delta > 2^a(r+1)^{2r+2}$ 有 $|\beta^{(n)}| \leqslant a(n+1)n(2n)^{a-1}(a-1)!2^{na}(r+1)^{2(r+1)n} = O(\delta^n)$.

由此得到推论. □

为了证明命题 E.2.2, 我们将 $F_n(X)$ 写成如下的样子:

$$F_n(X) = \prod_{i=1}^a \frac{n!P_i(X)}{X(X+1)\cdots(X+n)},$$

其中 P_i 是由

$$P_i(X) = \begin{cases} \binom{X-1-(i-1)n}{n}, & \text{如果 } 1 \leqslant i \leqslant r, \\ \binom{X+(i-r+1)n}{n}, & \text{如果 } r+1 \leqslant i \leqslant 2r, \\ 1, & \text{如果 } 2r+1 \leqslant i \leqslant a \end{cases}$$

定义的. ($\binom{X}{n}$ 是二项式形式的多项式 $\frac{X(X+1)\cdots(X-n+1)}{n!}$.)

我们需要几个预备性的结果.

引理 E.2.4. — 设 $Q \in \mathbf{Q}[X]$ 为次数 $\leqslant n$ 的在整数上取整数值的多项式, 且设 $(\beta_j(Q))_{0\leqslant j\leqslant n}$ 由如下的有理分式分解成简单分式时定义:

$$F(X) = \frac{n!Q(X)}{X(X+1)\cdots(X+n)} = \sum_{j=0}^n \frac{\beta_j(Q)}{X+j},$$

而令 $B(Q) = \sup_{0\leqslant j\leqslant n}|\beta_j(Q)|$. 于是对于任意的 $j \in \{0, \ldots, n\}$ 有 $\beta_j \in \mathbf{Z}$ 以及 $B(Q) \leqslant 2^n \sup_{0\leqslant j\leqslant n}|Q(-j)|$.

证明 我们有

$$\beta_j(Q) = \lim_{X\to -j}(X+j)F(X) = (-1)^j\binom{n}{j}Q(-j).$$

□

引理 E.2.5. — 设 $\mathbf{Q}_i, 1 \leqslant i \leqslant a$ 是在整数上取整数值的 $\leqslant n$ 的多项式. 设 $\alpha_{j,k}$, $0 \leqslant j \leqslant n, 1 \leqslant k \leqslant a$ 是由以下的分解为简单分式的公式确定的数:

$$F(X) = \prod_{i=1}^{a} \frac{n!Q_i(X)}{X(X+1)\cdots(X+n)} = \sum_{j=0}^{n}\sum_{k=1}^{a} \frac{\alpha_{j,k}}{(X+j)^k}.$$

于是 $d_n^{a-k}\alpha_{j,k} \in \mathbf{Z}$ 且对每个 $0 \leqslant j \leqslant n, 1 \leqslant k \leqslant a$ 有 $|\alpha_{j,k}| \leqslant (2n)^{a-1}(a-1)! \prod_{i=1}^{a} B(Q_i)$.

[500] 证明 证明由对 a 的归纳进行. $a=1$ 的情形包含在引理 E.2.4 中. 如果 $a \geqslant 2$, 归纳假设使我们可以写出

$$\prod_{i=1}^{a-1} \frac{n!Q_i(X)}{X(X+1)\cdots(X+n)} = \sum_{j=0}^{n}\sum_{k=1}^{a-1} \frac{\gamma_{j,k}}{(X+j)^k},$$

其中 $d_n^{a-1-k}\gamma_{j,k} \in \mathbf{Z}$ 且 $|\gamma_{j,k}| \leqslant (2n)^{a-2}(a-2)! \prod_{i=1}^{a-1} B(Q_i)$.

现在, 如果 $j_1 \neq j_2$, 则有

$$\frac{1}{(X+j_1)(X+j_2)^\ell} = \frac{1}{(j_2-j_1)^\ell (X+j_1)} - \sum_{k=1}^{\ell} \frac{1}{(j_2-j_1)^{\ell+1-k}(X+j_2)^k}.$$

由此得到公式

$$\alpha_{j,k} = \begin{cases} \beta_j(P_a)\gamma_{j,k-1} - \sum\limits_{\ell \geqslant k}\sum\limits_{j' \neq j} \dfrac{\beta_{j'}(P_a)\gamma_{j,\ell}}{(j-j')^{\ell+1-k}}, & \text{如果 } k \geqslant 2, \\ \sum\limits_{\ell \geqslant 1}\sum\limits_{j' \neq j} \dfrac{\beta_j(P_a)\gamma_{j',\ell} - \beta_{j'}(P_a)\gamma_{j,\ell}}{(j-j')^\ell}, & \text{如果 } k = 1. \end{cases}$$

右端的和最多包含了 $2n(a-1)$ 项, 而这些项中的每一个的绝对值都 $\leqslant B(P_a)(2n)^{a-2}(a-2)! \prod_{i=1}^{a-2} B(P_i)$; 由此我们得到想要的对于 $|\alpha_{j,k}|$ 的强函数.

最后, 我们有

$$d_n^{a-k} \frac{\beta_{j'}(P_a)\gamma_{j,k}}{(j-j')^{\ell+1-k}} = d_n^{a-1-\ell}\gamma_{j,\ell} \cdot \frac{d_n^{\ell+1-k}}{(j-j')^{\ell+1-k}} \cdot \beta_{j'}(P_a) \in \mathbf{Z}$$

和

$$d_n^{a-k}\gamma_{j,k-1} = d_n^{a-1-(k-1)}\gamma_{j,k-1} \in \mathbf{Z},$$

从而涉及计算 $\alpha_{j,k}$ 的每一项均为整数; 故由此知 $\alpha_{j,k}$ 也是整数. 证完. □

引理 E.2.6. — 如果 $1 \leqslant i \leqslant a$, 则 P_i 是在整数上取值为整数的次数 $\leqslant n$ 的多项式. 另外, 我们有

$$B(P_i) \leqslant \begin{cases} 2^n \dfrac{((i+1)n)!}{(in)!n!}, & \text{如果 } 1 \leqslant i \leqslant r, \\ 2^n \dfrac{((i-r+1)n!)}{((i-r)n)!n!}, & \text{如果 } r+1 \leqslant i \leqslant 2r, \\ 2^n, & \text{如果 } 2r+1 \leqslant i \leqslant a. \end{cases}$$

证明 $\binom{X}{n}$ 在整数上取整数值 (参看小词典的 §1.1), 由此知 P_i 也如此. 然而, 从二项式系数 $\binom{n}{j}$ 以 2^n 为强函数, 并注意到 $|P_i(-j)|, 0 \leqslant j \leqslant n$ 的最大值当 $1 \leqslant i \leqslant r$ (分别地, $r+1 \leqslant i \leqslant 2r$) 在 $j=0$ (分别地, $j=n$) 达到, 则引理中 $B(P_i)$ 的强函数可由此得到. □

命题 E.2.2 是引理 E.2.6 和 E.2.5 以及下面的强函数关系的推论:

$$\prod_{i=1}^{a} B(P_i) \leqslant 2^{na}\left(\frac{((r+1)n)!}{(n!)^{r+1}}\right)^2 \leqslant 2^{na}(r+1)^{2(r+1)n}.$$

第一个不等式由将引理 E.2.6 的那些强函数相乘得到, 而第二个不等式则利用了多重项式的系数的强函数得到 (如果 $m_1+\cdots+m_c=m$, 则 $\frac{m!}{m_1!\cdots m_c!}$ 是 $(x_1+\cdots+x_c)^m$ 的展开式中 $x_1^{m_1}\cdots x_c^{m_c}$ 的系数, 从而 $\leqslant c^m$(令 $x_1=\cdots=x_c=1$): 这个系数是 $\{1,\ldots,m\}$ 分拆为 c 个集合的个数, 具有 m_1 个元的第一个对应因子 x_1 所处的位置, 具有 m_2 个元的第二个则对应了 $\cdots\cdots$; 然而置换群 S_m 置换这些分拆, 而 $\sigma \in S_m$ 让一个分拆不动当且仅当它让此分拆中每一个集合都不动; 由此推出一个这样的分拆 p 的一个稳定子 G_p 具有基数 $m_1!\cdots m_c!$, 因此这些分拆的个数等于 $\frac{|S_m|}{|G_p|}=\frac{m!}{m_1!\cdots m_c!}$). [501]

4. S_n 的估值

S_n[46]的一个积分形式 (命题 E.2.9) 让我们可以研究 S_n 的渐近行为: 可得到如下结果:

命题 E.2.7. — (i) 存在 $A_0>0$ 使得 $\lim_{n\to+\infty} S_n^{1/n}=A_0$.

(ii) 有 $A_0 \leqslant (2r+1)^{2r+1}r^{2r-a}$.

引理 E.2.8. — 如果 $a,b\in\mathbf{N}$, 则 $\int_0^1 x^a(1-x)^b dx=\frac{a!b!}{(a+b+1)!}$.

证明 它是欧拉公式 $\int_0^1 x^{s-1}(1-x)^{t-1}dx=\frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}$ 的特殊情形 (我们也可利用公式 $\int_0^1 x^a(1-x)^b dx=\frac{b}{a+1}\int_0^1 x^{a+1}(1-x)^{b-1}dx$.) □

命题 E.2.9. — 我们有

$$S_n=\frac{((2r+1)n+1)!}{(n!)^{2r+1}}\int_{[0,1]^{a+1}}\frac{\prod_{\ell=1}^{a+1} x_\ell^{nr}(1-x_\ell)^n dx_\ell}{(1-x_1\cdots x_{a+1})^{(2r+1)n+2}}.$$

证明 如果 $k\geqslant 1$ 及 $|x|<1$, 则有 $(1-x)^{-k}=\sum_{m=0}^{+\infty}\binom{m+k-1}{k-1}x^m$. 由于考虑中的这些函数都是正的, 故可交换求和与积分运算从而得到

$$\begin{aligned}\int_{[0,1]^{a+1}}\frac{\prod_{\ell=1}^{a+1}(x_\ell^{nr}(1-x_\ell)^n dx_\ell)}{(1-x_1\cdots x_{a+1})^k} &= \sum_{m=0}^{+\infty}\binom{m+k-1}{k-1}\left(\int_0^1 x^{rn+m}(1-x)^n dx\right)^{a+1}\\ &= \sum_{m=0}^{+\infty}\frac{(m+1)\cdots(m+k-1)}{(k-1)!}\left(\frac{(rn+m)!n!}{((r+1)n+m+1)!}\right)^{a+1}.\end{aligned}$$

[46]注意, 这不是置换群而是前面第 2 小节的那些有理分式值 $F_n(m)$ 的和.

对于 $k=(2r+1)n+2$, 我们有

$$\frac{((2r+1)n+1)!}{(n!)^{2r+1}}\frac{(m+1)\cdots(m+k-1)}{(k-1)!}\left(\frac{(rn+m)!n!}{((r+1)n+m+1)!}\right)^{a+1}=F_n(rn+m+1).$$

由于当 $1\leqslant m\leqslant rn$ 时 $F_n(m)=0$, 故得出结果. □

引理 E.2.10. — 我们有

$$\lim_{n\to+\infty}\left(\frac{((2r+1)n+1)!}{(n!)^{2r+1}}\right)^{1/n}=(2r+1)^{2r+1}.$$

[502] 证明　这是由斯特林公式 $n!=n^ne^{-n}\sqrt{2\pi n}(1+O(\frac{1}{n}))$ (参看命题 VII.2.9) 给出的 $n!$ 的渐进行为的一个推论. □

引理 E.2.11. — 设 $K\subset\mathbf{R}^{a+1}$ 为一紧集, f 是 K 上的一个连续函数, 而 $g\in L^1(K)$ 是一个正函数并且它在 K 的每个开集上的积分非零. 于是 $\lim_{n\to+\infty}|\int_K f^ngdx|^{1/n}=\sup_{x\in K}f(x)$.

证明　令 $M=\sup_{x\in K}f(x)$ 且 $I_n=\int_K f^ngdx$.

- 对所有的 $n\gg0$ 以及 $\varepsilon>0$, 我们有 $I_n\leqslant M^n\int_K gdx$, 从而 $I_n^{1/n}\leqslant(1+\varepsilon)M$.
- f 在某个点 $u\in K$ 达到它的最大值 M, 因此对于所有的 $\varepsilon>0$ 存在一个包含 u 的开集 $U\subset K$, 使得对所有 $x\in U$ 有 $f(x)\geqslant M-\varepsilon$. 于是 $I_n\geqslant(M-\varepsilon)^n\int_U gdx$, 又由于 $\int_U gdx>0$, 故对 $n\gg0$ 有 $I_n^{1/n}\geqslant(1-\varepsilon)(M-\varepsilon)$.

由此得到, 当 $n\to+\infty$ 时 $I_n^{1/n}\to M$, 即为所求. □

转到命题 E.2.7 的证明. 将引理 E.2.10 和 E.2.11 用于 $K=[0,1]^{a+1}$, $f(x)=\frac{\prod_{\ell=1}^{a+1}x_\ell^r(1-x_\ell)}{(1-x_1\cdots x_{a+1})^{2r+1}}$ 和 $g(x)=\frac{1}{(1-x_1\cdots x_{a+1})^2}$ 证明了

$$\lim_{n\to+\infty}S_n^{1/n}=A_0,$$

其中

$$A_0=(2r+1)^{2r+1}\sup_{x\in[0,1]^{a+1}}f(x).$$

另一方面, 对于每个 $\ell\in\{1,\ldots,a+1\}$, 我们有 $1-x_1\cdots x_{a+1}\geqslant1-x_\ell$. 因此也有 $1-x_1\cdots x_{a+1}\geqslant\prod_{\ell=1}^{a+1}(1-x_\ell)^{1/(a+1)}$, 由此有强函数 $f(x)\leqslant\prod_{\ell=1}^{a+1}(x_\ell(1-x_\ell)^{\frac{a-2r}{a+1}})$. $x\mapsto x^r(1-x)^{\frac{a-2r}{a+1}}$ 在 $[0,1]$ 上的最大值在 $\rho=(1+\frac{a-2r}{r(a+1)})^{-1}$ 达到; 因此 f 在 $[0,1]^{a+1}$ 上的最大值 $\leqslant\rho^{r(a+1)}(1-\rho)^{a-2r}\leqslant(1-\rho)^{a-2r}$, 那么由于强函数关系

$$1-\rho=1-\frac{1}{1+\frac{a-2r}{r(a+1)}}=\frac{\frac{a-2r}{r(a+1)}}{1+\frac{a-2r}{r(a+1)}}\leqslant\frac{a-2r}{r(a+1)}\leqslant\frac{1}{r},$$

便最后得到命题 E.2.7 的证明.

5. Nesterenko 判别法的应用

5.1. 前 n 个整数的最小公倍数

为了应用 Nesterenko 判别法我们需要估计 d_n 的大小.

命题 E.2.12. — 存在 $\gamma > 1$ 使得 $d_n = O(\gamma^n)$.

证明 整除 d_n 的素数只是那些 $\leqslant n$ 的, 而如果 $p^v \mid b \leqslant n$, 则 $v \leqslant [\frac{\log n}{\log p}]$, 从而 $v_p(d_n) = [\frac{\log n}{\log p}]$. 由此得到

$$\log d_n \leqslant \sum_{p \leqslant n} [\frac{\log n}{\log p}] \log p \leqslant \pi(n) \log n,$$

其中 $\pi(n) = |\{p \in \mathscr{P}, p \leqslant n\}|$. 素数定理 ($\pi(n) \sim \frac{n}{\log n}$) 表明, 对于 $n \gg 0$ 有 $\log d_n \leqslant \alpha n$, 其中 $\alpha > 1$; 因此我们可取任意的 $\gamma > e$. (利用在 $m+1$ 和 $2m$ 之间的素数的乘积整除 $\binom{2m}{m} \leqslant 2^{2m}$ 这个事实可以证明 $\gamma > 4$(习题) 而不需要借助素数定理.) [503] □

5.2. 由这些 $\zeta(2j+1)$ 生成的 $\mathbf{Q}$-向量空间的维数的下界

我们的努力因以下的命题得到了回报, 这个命题给出了由 ζ 函数在奇数或者在偶数上的值生成的 $\mathbf{Q}$-向量空间的维数的一个下界估计.

命题 E.2.13. — 设 $a \geqslant 3$ 为一个奇整数. 设 $\delta_{\text{pair}}(a)$ (分别地, $\delta_{\text{impair}}(a)$) 是由 1 和那些 k 为偶数 (分别地, 奇数) 时的 $\zeta(k), 2 \leqslant k \leqslant a$ 生成的 $\mathbf{R}$ 的 $\mathbf{Q}$– 线性子空间的维数. 于是对于任意的 $r \leqslant \frac{a}{2}$, 维数 $\delta_{\text{pair}}(a)$ 和 $\delta_{\text{impair}}(a)$ 都被

$$1 + \frac{(a-2r)\log r - a\log\gamma - (2r+1)\log(2r+1)}{a\log 2\gamma + (2r+2)\log(r+1)}$$

囿于下.

注记 E.2.14. — 取 $r = \frac{a}{(\log a)^2} + O(1)$, 则看出 $\delta_{\text{pair}}(a)$ 和 $\delta_{\text{impair}}(a)$ 被 $1 + \frac{\log a}{\log 2\gamma} + o(1)$ 囿于下; 特别地, $\delta_{\text{pair}}(a)$ 和 $\delta_{\text{impair}}(a)$ 趋向 $+\infty$, 这便完成了定理 E.1.1 的证明 (mod 本命题的证明).

证明 对于 $\delta_{\text{pair}}(a)$ 的证明与对 $\delta_{\text{impair}}(a)$ 的证明是一样的 (但稍微简单一点); 所以我们只处理 $\delta_{\text{impair}}(a)$ 的情形.

设 D_n 是 d_n 的某个倍数使得 $D_n = \gamma^{n+o(n)}$, 其中的 γ 满足命题 E.2.12 的结论. 令 $b = \frac{a+1}{2}$, $v_1 = 1$ 而 $v_j = \zeta(2j-1), 2 \leqslant j \leqslant b$. 又设 $a_{n,1} = D_{2n+1}^a \beta^{(2n+1)}$ 及 $a_{n,j} = D_{2n+1}^a \alpha_{2j-1}^{(2n+1)}, 2 \leqslant j \leqslant b$. 根据命题 E.2.3, 这些 $a_{n,j}$ 是整数, 而命题 E.2.12 和推论 E.2.3 的 (ii) 合起来证明了

$$\sup_{1 \leqslant j \leqslant b} |a_{n,j}| = O(B^n),$$

从而对于所有的 $B > (\gamma^a 2^a (r+1)^{2r+2})^2$ 有

$$\sum_{1\leqslant j\leqslant b} |a_{n,j}| \leqslant B^{n+o(n)}.$$

另一方面, 因为当 k 为偶数时 $\alpha_k^{(2n+1)} = 0$, 故对奇数 a, 我们有 $a_{n,1}v_1 + \cdots + a_{n,b}v_b = D_{2n+1}^a S_{2n+1}$. 命题 E.2.7 和 E.2.12 的结合证明了存在 $A > 0$ 使得

$$|a_{n,1}v_1 + \cdots + a_{n,b}v_b| = A^{-n+o(n)},$$

其中

$$A \geqslant (\gamma^a (2r+1)^{2r+1} r^{2r-a})^2.$$

因此 Nesterenko 判别法 (定理 E.1.3) 让我们得到了结论. □

附录 F. 同余数问题

本章通过至今仍未解决的古老的同余数问题来介绍伯奇与斯温纳顿–戴尔猜想 (la conjecture of Birch et Swinnerton-Dyer, 简称 BSD 猜想)(这是一个悬赏百万美元的问题).

F.1. 椭圆曲线与同余数

1. 问题的引进

定义 F.1.1. — 设 D 是一个无平方因子的整数 (即不被任意素数的平方整除的数), 称它是个同余数是说, 存在一个有理数边长的直角三角形其面积是 D; 换言之, 当且仅当存在 $a, b, c \in \mathbf{Q}$ 满足 $a^2 + b^2 = c^2$ 和 $D = \frac{ab}{2}$.

为了研究同余数问题, 我们从研究具有有理数边的直角三角形的集合着手, 就是说, 在有理数中解方程 $a^2 + b^2 = c^2$. 令 $u = \frac{a}{c}, v = \frac{b}{c}$, 于是化成寻找圆 $u^2 + v^2 = 1$ 上 $u > 0, v > 0$ 的有理点的问题了. 为此, 以 t 记 (u, v) 与 $(-1, 0)$ 联结直线的斜率, 故此直线的方程为 $v = t(u + 1)$; 我们有 $t \in \mathbf{Q}$ 以及 $(u, v) = (\frac{1-t^2}{t^2+1}, \frac{2t}{t^2+1})$. 总起来说, $a, b, c \in \mathbf{Q}$ 是一个直角三角形的边当且仅当存在 $t \in \mathbf{Q}, 0 < t < 1$, 使得 $a = \frac{1-t^2}{t^2+1}c$, $b = \frac{2t}{t^2+1}c$. 令 $x = -t, y = \frac{t^2+1}{c}$, 那么前面所叙述的几乎[1] 可以证明以下

[1]关系 $D = \frac{ab}{2}$ 成了 $D = \frac{x^3-x}{y^2}$, 而条件 $0 < t < 1$ 则等价于 $-1 < x < 0$. 因此我们已经证明了 D 是同余数当且仅当方程 $Dy^2 = x^3 - x$ 有在 $\mathbf{Q}^2$ 中满足 $-1 < x < 0$ 的一个解. 曲线 $C_D(\mathbf{R}) = \{(x, y) \in \mathbf{R}^2, Dy^2 = x^3 - x\}$ 有两个连通分支: 一个是在 $-1 \leqslant x \leqslant 0$ 中的卵形线, 而另一个是在区域 $x \geqslant 1$ 中具有竖直渐进方向的曲线. 将 $P = (x, y)$ 映到 $P' = (x', y')$ 的映射, 即直线 $(P, (-1, 0))$ 与 C_D 的交点, 交换了两个连通分支, 这可从作一下图 (或显式地计算) 就可看出, 并且如在 §2 中解释的那样 (或经显式计算表明), 它将 $C_D(\mathbf{Q})$ 带到了自己. 这让我们可以证明在 $\mathbf{Q}^2$ 中存在一个满足 $-1 < x < 0$ 的解等价于在 $\mathbf{Q}^2$ 中存在一个满足 $x > 1$ 的解. 由此得到了命题.

[506] 的命题, 它建立了同余数问题与一些丢番图方程之间的联系 (参看 §F.2.).

命题 F.1.2. — 如果 D 是个无平方因子的正整数, 则下面的条件等价:

(i) D 是同余数.

(ii) 方程 $Dy^2 = x^3 - x$ 在 $\mathbf{Q}^2$ 中有 $y \neq 0$ 的一个解.

决定一个整数是否是同余数是一个非常古老也是非常困难的问题. 例如, 我们有下面斐波那契 (Fibonacci, 1175—1240) "猜想" 的结果.

定理 F.1.3. — (费马, 1601—1665) 1 不是同余数.

这是费马为他的 "无限下降法[2]" 找到的众多应用之一. 我们注意到, 如果 a, b, c 满足 $a^4 - b^4 = c^4$, 并且如果 $x = \frac{a^2}{b^2}, y = \frac{ac^2}{b^3}$, 则有 $y = x^3 - x$. 1 不是同余数的事实因此蕴含了费马对于指数 4 的定理[3].

例题 F.1.4. — (Zagier) 157 是个同余数, 但面积为 157 的最简单的三角形 (a, b, c) 是

$$a = \frac{6803298487826435051217540}{411340519227716149383203}, \quad b = \frac{411340519227716149383203}{21666555693714761309610},$$

$$c = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

这个例子表明找寻面积为 D 的有理数边的直角三角形有点像要杂技一样冒险.

定理 F.1.5. — 设 D 是个无平方因子的奇整数. 如果 D 是个同余数, 则

$$|\{x, y, z \in \mathbf{Z}, 2x^2 + y^2 + 8z^2 = D\}| = 2 \cdot |\{x, y, z \in \mathbf{Z}, 2x^2 + y^2 + 32z^2 = D\}|. \quad (*)$$

反之, 如果 D 满足 $(*)$, 且若 (一个弱形式的)BSD 猜想为真, 则 D 是同余数.

对于 D 是偶整数的情形有类似的结果. 由于决定 D 是否满足 $(*)$ 是非常容易的事[4], 这提供了可以决定一个给定的数不是同余数或者 (在 BSD 假设下) 是同余数. 一个 mod 8 同余于 5 或 7 的数满足 $(*)$: 因为这两个集合都为空集, 但是我们不知道如何证明这蕴含了 D 是个同余数 …….

[507] 正如读者将看到的, 这个定理的证明借助了一条非常迂回曲折的道路 (正是它的魅力所在); 人们可能有点想问是否能有一个更直接的证明, 现在我们将要知道答案了.

2. 椭圆曲线的算术

如果 C 是一条圆锥线, 我们可以研究 C 的具有有理坐标的点的集合 $C(\mathbf{Q})$, 就像我们在圆上那样. 我们找出圆锥线上的一个点 $P \in C(\mathbf{Q})$ 然后作一条通过 P 的变化

[2] 这个方法构成了问题 H.14 的内容; 将此问题特殊到 $D = 1$ 情形, 我们便得到了费马结果的一个证明 (只需要部分的 III 和 IV).

[3] 似乎费马对此问题的热情有点过度.

[4] 读者可以从推演定理 F.1.3 的过程中得以确信.

的直线并以此来对圆锥线上的点进行参数化. 这个方法对于由一个三次方程给出的曲线则不能继续使用 (像是对由方程 $Dy^2 = x^3 - x$ 给出的曲线 C_D), 这是因为, 如果我们用通过 $C(\mathbf{Q})$ 的一条直线去切割, 并从两个方程中消去 y, 便得到一个 x 的 3 次方程, 而我们只知道其中有一个解是有理的; 因此另外两个解, 一般来说, 在 $\mathbf{Q}$ 的一个二次扩域中, 而不在 $\mathbf{Q}$ 中. 然而, 如果取一条通过 C 的两个有理点的直线或在一个有理点的切线, 则得到其两个解 (或一个二重解) 是有理数的方程; 因为根的和是有理的, 故此直线切割 C 在另一个有理点.

在一个域 K 上的椭圆曲线[5]是方程为 $y^2 = P(x)$ 的曲线 (如图 1), 其中 $P \in K[X]$ 是 3 次的无重根的多项式[6]. 以 $E(K)$ 记 $y^2 = P(x)$ 在 K^2 中解的集合, 而 $\overline{E}(K) = E(K) \cup \{\infty\}$, 按约定, 一条直线通过 ∞ 当且仅当它是竖直的[7]. 赋予 $\overline{E}(K)$ 一个合成律 $+$, 它实际上是一个以 ∞ 为中性元的交换群[8], 并且 $P + Q + R = \infty$ 当且仅当 (P, Q, R) 三点共线 (在其中两个或三个点分不开时我们有显然的约定; 特别 P 是 2 阶的当且仅当 ∞ 属于 E 在 P 的切线, 就是说直线 $y = 0$; 同样, P 是 3 阶的当且仅当 E 在 P 的切线有 3 阶接触).

定理 F.1.6. — *如果 E 是 $\mathbf{Q}$ 上的一条椭圆曲线, 则群 $\overline{E}(\mathbf{Q})$ 由有限个元生成; 因此它同构于 $\overline{E}(\mathbf{Q})_{\text{tors}} \oplus \mathbf{Z}^{r(E)}$, 其中 $\overline{E}_{\text{tors}}$ 是具有限阶的点的子群[9], 它是一个有限群, 而 $r(E) \in \mathbf{N}$.* [508]

这个结果被庞加莱在 1900 年左右猜想出来过, 而由莫德尔在 1922 年证明, 他采用了费马的无限下降法[10]: 这是著名的莫德尔–韦伊定理的一个特殊情形. 群 $\overline{E}(\mathbf{Q})_{\text{tors}}$ 极容易计算; 相反地, 秩 $r(E)$ 和 $\mathbf{Z}^{r(E)}$ 的生成元的确定却是个非常精致的工作, 迄今为止, 仍然没有证明有一个可以确定它们的算法; 虽然它对于与我们的同余数相关的问题没有多少帮助, 但是我们以后将要讨论的 BSD 猜想如果能够被证明, 却可提供出这样一个算法.

例题 F.1.7. — 以 C_D 记方程为 $Dy^2 = x^3 - x$ 的椭圆曲线. 则 $Q_1 = (-1, 0), Q_2 = (0, 0), Q_3 = (1, 0)$ 都是 2 阶的, 而 $\overline{C}_D(\mathbf{Q})_{\text{tor}} = \{\infty, Q_1, Q_2, Q_3\}$. 结论是, D 为同余数

---

[5] 如果 K 为特征 2 的, 也应该可以有 $y^2 + y = P(x)$ 类型的曲线.

[6] 这等于是说 P 的判别式 $\Delta(P)$ 不为零 (参看小词典的 9.2.1 小节).

[7] $\overline{E}(K)$ 的这个定义完全是人为的. 一个自然的定义要求在射影平面 $\mathbf{P}^2$, 即 3 维向量空间中的直线的空间中进行. 它可以看作是仿射平面和一条在无限远处的 (射影) 直线的并, 而这个无限远直线上的点对应于仿射平面中直线的方向; ∞ 是一条到无限远的竖直直线的方向对应的点.

[8] 结合律不是显然的. 可以用一个十分繁复的显式计算来证明它 (但可以要求计算机的帮助 ……). 一个更简洁的解决办法是, 如果 K 是 $\mathbf{C}$ 的子域, 则转到用椭圆函数 (参看问题 H.8), 这让我们证明 $\overline{E}(\mathbf{C})$ 作为群同构于 $\mathbf{C}/\Lambda$, 其中 Λ 是 $\mathbf{C}$ 的一个格 (为了能应用问题 H.8 的结果, 必须知道 $X^3 - aX - b$ 的判别式是否不为 0 以及是否存在 $\mathbf{C}$ 的一个格 Λ 使得 $g_2(\Lambda) = a$ 和 $g_3(\Lambda) = b$; 利用模不变量 j 的满性 (习题 VII.6.7) 和 g_2 与 g_3 的齐次性, 它可使 g_2 和 g_3 表达为 G_4 和 G_6 的函数). 在一般情形有通过射影几何的漂亮证明.

[9] 如果 K 是 $\mathbf{C}$ 的一个子域, 且若 $\overline{E}(\mathbf{Q}) \cong \mathbf{C}/\Lambda$, 则 $\overline{E}(K)$ 的 n-挠点的子群等同于 $\frac{1}{n}\Lambda/\Lambda \cong (\mathbf{Z}/n\mathbf{Z})^2$ 的一个子群; 特别地, 它的基数 $\leqslant n^2$.

[10] C_D 的特殊情形是问题 H.14 的内容.

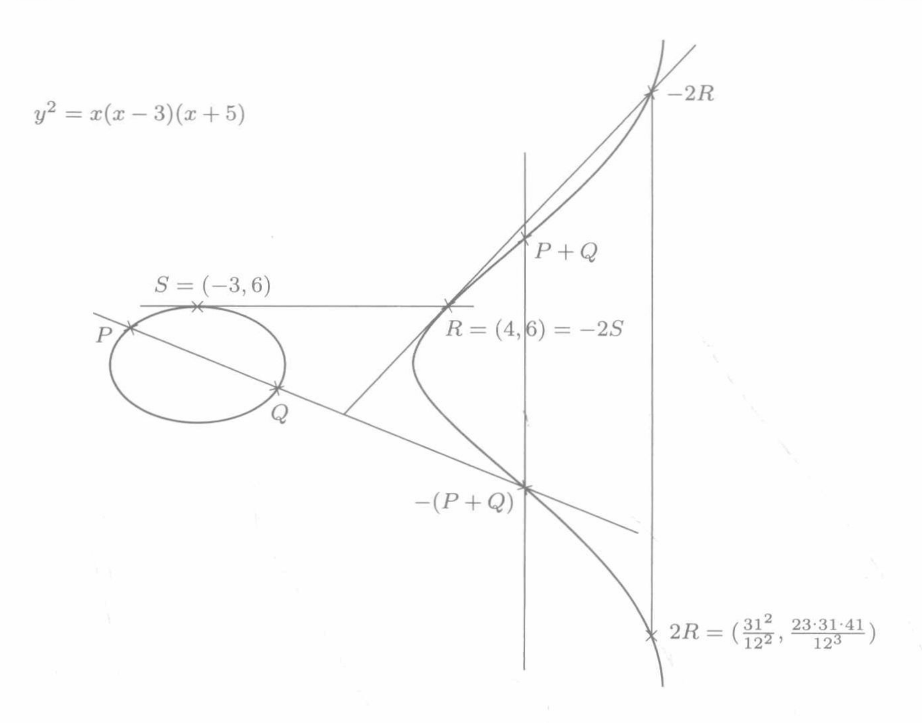


图 1. 方程 $y^2 = x(x-3)(x+5)$ 定义的椭圆曲线上的加法

当且仅当 $r(C_D) \geqslant 1$.

[509] 3. 伯奇与斯温纳顿–戴尔的探索

如果 p 是个素数, 于是 $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ 是一个域. 如果 $r = \frac{a}{b} \in \mathbf{Q}$, 而 p 不整除 b, 于是 a 和 b 的 $\bmod p$ 约化则可将 r 看为 F_p 中的元 (即取 a 和 b 在 F_p 中的像的商, 这不依赖 a 和 b 的选取). 特别地, 如果 E 是 $\mathbf{Q}$ 上方程 $y^2 = P(x)$ 的椭圆曲线, 则也可将 E 想成是对所有好素数的 $\mathbf{F}_p$(即既不整除 P 的系数的分母也不整除它的判别式的分子 (脚注 6)) 上的椭圆曲线.

如果 E 是 $\mathbf{F}_p$ 上的一条椭圆曲线[11], 我们则显然有 $|\overline{E}(\mathbf{F}_p)| \leqslant 2p+1$, 但我们还是给出以下的更精确的结果.

定理 F.1.8. — (哈塞 (Hasse), 1933) 如果 E 是 $\mathbf{F}_p$ 上的一条椭圆曲线, 且若令 $a_p = p+1-|\overline{E}(\mathbf{F}_p)|$, 则 $|a_p| \leqslant 2\sqrt{p}$.

伯奇与斯温纳顿–戴尔 (1960—1965) 的想法是, 由于 $E(\mathbf{Q})$ 中点经过了 $\bmod p$ 约化, 故当 $r(E) \geqslant 1$ 时, $E(\mathbf{F}_p)$ 中的点平均来说应该比当 $r(E)=0$ 时更多. 而根据哈塞定理, 这个点的个数更靠近 p 一点, 故当 $r(E) > 1$ 时, 乘积 $\prod_p \frac{p}{|E(\mathbf{F}_p)|}$ 应该有发散

[11] 我们也可考虑 $\mathbf{Z}/D\mathbf{Z}$ 上的椭圆曲线, 其中 D 不是素数, 或者在 $\mathbf{F}_q$ 上. 这对于大数分解因子, 证明大数的素性, 或者对于建立其大小等于由 $\mathbf{F}_q^*$ 给出的最可信签名方面是有用的.

(为零) 的可能, 而当 $r(E)=0$ 时, 则有收敛的可能. 由于这个乘积在通常意义下不收敛, 故我们应该通过全纯函数以便把这种探索具体化.

4. 椭圆曲线的 L 函数

设 E 是 $\mathbf{Q}$ 上的椭圆曲线. 如果 p 是一个好的素数, 那么, 设 a_p 是由 $a_p = 1+p-|\overline{E}(\mathbf{F}_p)|$ 定义的整数. 我们定义函数 $L(E,s)$[12] 以及对于每个 $n \in \mathbf{N}-\{0\}$ 的整数 a_n 为

$$L(E,s) = \prod_{p\text{为好素数}} \frac{1}{1-a_p p^{-s}+p^{1-2s}} = \sum_{n=1}^{+\infty} a_n n^{-s}.$$

容易看出这个乘积对 $\mathrm{Re}(s)>2$ 收敛, 而如果用哈塞的囿于上强函数 $|a_p| \leqslant 2\sqrt{p}$, 则 $\mathrm{Re}(s)>\frac{3}{2}$ 也同样收敛, 从而在这个半平面上定义了一个全纯函数.

定理 F.1.9. — *函数 $L(E,s)$ 有一个到整个 $\mathbf{C}$ 的解析延拓.* [510]

哈塞在 1935 年间就已猜出了这个结果; 这是哈塞–韦伊猜想的一个特殊情形. 在此方向上的第一个成果是属于韦伊 (1952) 关于曲线族 C_D 的[13]. 而志村五郎 (Shimura, 1958) 受到艾克勒 (Eichler, 1952) 工作的激励, 证明了这个猜想的许多情形, 为此, 他利用了我们以后要讨论的模形式的理论. 最重要的步骤则由怀尔斯在 1994 年完成, 在追寻费马大定理的证明中, 他证明了在 E 是方程 $y^2=P(x)$ 而 P 的所有根均在 $\mathbf{Q}$ 中的情形中的这个猜想. 一般情形最后由 Breuil, Conrad, Diamond 和 Taylor 在 1999 年解决.

在伯奇与斯温纳顿–戴尔的探索中出现的 $\prod_{p\text{为好素数}} \frac{p}{|\overline{E}(\mathbf{F}_p)|}$ 等于, 至少在形式上等

---

[12]这个函数并不是我们习惯上所考虑的那个函数; 它与其相差一个坏 p 的乘法因子, 但由于在 $s=1$ 不为零, 它没有改变 BSD 猜想所关切的东西. 这个好的函数 $L(E,s)$ 有一个在下面文字中考虑的好的函数方程, 存在 $\varepsilon \in \{\pm 1\}$ 和 $N \in \mathbf{N}$ 使得, 如果 $\Lambda(E,s) = \frac{\Gamma(s)}{(2\pi)^s} N^{s/2} L(E,s)$, 则 $\Lambda(E,2-s) = \varepsilon\Lambda(E,s)$; 特别地, 如果 $\varepsilon=-1$, 则 $r_\infty(E)$ 是奇数并且 $L(E,1)=0$.

[13]在这个情形, 我们定义 $\delta : \mathbf{Z}[i] \to \{0,1,i,-1,-i\}$ 为

$$\begin{cases} \delta(\omega)=0, & \text{如果 } \omega \text{ 在 } \mathbf{Z}[i] \text{ 中被 } 1+i \text{ 整除}, \\ \omega\delta(\omega)-1 \text{被 } (1+i)^3 \text{ 整除}, & \text{其他}. \end{cases}$$

于是有

$$L(C_1,s) = \frac{1}{4} \sum_{\omega \in \mathbf{Z}[i]-\{0\}} \frac{\omega\delta(\omega)}{|\omega|^{2s}} = \sum_{n=1}^{+\infty} a_n n^{-s}.$$

一般 D 的情形容易化成 $D=1$ 的情形: 我们有 $L(C_D,s)=\sum_{n=1}^{+\infty} \chi_D(n) a_n n^{-s}$, 其中 $\chi_D : \mathbf{Z} \to \{-1,0,1\}$ 是 mod D 的勒让德符号. 这个勒让德符号被如下的性质刻画: $\chi_D(n+4D)=\chi_D(n)$, 当 $(D,n) \neq 1$ 时 $\chi_D(n)=0$ 以及

$$\chi_D(nm)=\chi_D(n)\chi_D(m), \quad \chi_D(p) = \begin{cases} 1, & \text{如果 } D \text{ 在 } \mathbf{F}_p^* \text{ 中为平方}, \\ -1, & \text{如果 } D \text{ 在 } \mathbf{F}_p^* \text{ 中不为平方}. \end{cases}$$

χ_D 的存在性是欧拉在 1783 年猜测, 高斯在 1801 年证明的二次互反律的一个推论.

于 $L(E,1)$, 从而他们的探索成了:

猜想 F.1.10. — (伯奇与斯温纳顿–戴尔 (弱形式)) “$r(E) \geqslant 1$” 当且仅当 “$L(E,1)=0$”.

来把这个陈述精确化[14].

以 $r_\infty(E)$ 记 $L(E,s)$ 在 $s=1$ 的零点的阶. BSD 猜想于是具有以下形式.

猜想 F.1.11. — (伯奇与斯温纳顿–戴尔) 成立等式 $r(E)=r_\infty(E)$.

[511] 正是在这种形式下, 这个问题值 $1000,000. 事实上这个猜想有一个更加准确的形式[15] (给出了对 $\lim_{s\to1}(s-1)^{-r(E)}L(E,s)$ 的一个公式), 也更为一般 ($\mathbf{Q}$ 可以换成一个有限扩域, 甚至换成一个特征为 p 的域, 域 $\mathbf{F}_p(T)$ 的有限扩域).

只有如下的少许几个结果.

- 科兹和怀尔斯 (Coates-Wiles,1977) 证明了, 如果 $E=C_D$(或者如果 E 是 $\mathbf{Q}$ 上一条具有复乘的椭圆曲线 [16]), 于是, “$L(E,1)\neq 0$” ⇒ “$r(E)=0$”.
- 格罗斯和察基尔 (Gross-Zagier, 1983) 给出了 $L'(E,1)$ 的一个显式公式[17], 它通过称作 “西格勒尔 (Heegner) 点” 的 E 上的一些有理点表达, 而这些西格勒尔点可以以纯粹的解析方式构造出来 (它是那些可以让展示具有有理数边的直角三角形的展览馆兴高采烈的点, 因为这些有理数具有天文个数的字码), 作为推论, 他们得到了一个蕴含关系: “$r_\infty(E)=1$” ⇒ “$r(E)\geqslant 1$”.
- 科里瓦金 (Kolyvagin, 1989) 利用西格勒尔点证明了蕴含关系 “$r_\infty(E)\leqslant 1$” ⇒ “$r(E)=r_\infty(E)$”.

这就是全部! 我们处在了一个尴尬的矛盾境地, 越是觉得有有理点 ($r_\infty(E)\geqslant 2$) 就越不知道如何构造它 ······. 无论怎样, 我们还是要提到, 虽然一般地, 秩 $r(E)$ 等于 0 或者 1, 但有充分的理由相信 $r(E)$ 可以取任意大的值, 保持的最近记录是 Elkies (2006), 他给出了一条满足 $r(E)\geqslant 28$ 的曲线; Bhargava 和 Shankar (2011) 证明了平

---

[14] 事实上, 伯奇与斯温纳顿–戴尔更为乐观, 他们猜测

$$\prod_{p\text{为好素数},p\leqslant x}\frac{p}{|\overline{E}(\mathbf{F}_p)|}\sim C(\log x)^{-r(E)}.$$

哥德菲尔德 (Goldfeld, 1982) 证明了, 如果是这种情形, 那么 $r_\infty(E)=r(E)$, 而函数 $L(E,s)$ 则满足黎曼假设 (即它对 $\mathrm{Re}(s)>1$ 不取零值), 但令人惊奇的是, 当 $r(E)=0$ 时, 我们有 $C=\frac{L(E,1)}{\sqrt{2}}$ 而不是 $C=L(E,1)$.

[15] 它具有 $\lim_{s\to1}(s-1)^{-r(E)}L(E,s)=|\text{Ш}(E)|\cdot R_\infty(E)\cdot\Omega_\infty(E)\cdot\prod_{p\text{为坏的素数}}c_p$ 形式, 这里的 c_p 是一个有显式表达的有理数, $\Omega_\infty(E)$ 是 E 的实数周期 (当 E 由 $y^2=P(x)$ 给出时, $\Omega_\infty(E)=2\int_\alpha^{+\infty}\frac{dx}{\sqrt{P(x)}}$, 其中 α 是 P 的最大实根), $R_\infty(E)$ 是度量 $\overline{E}(\mathbf{Q})$ 的生成元大小的一个 “调整子”, 而 $\text{Ш}(E)$ 则是 E 的泰特–沙法列维奇 (Tate-Shafarevich) 群, 它是一个有点神秘的群, 猜测它是有限的.

[16] 如果 $(x,y)\in\mathbf{C}_D(\mathbf{C})$, 则 $(-x,iy)\in C_D(\mathbf{C})$. 如果 Λ 是对应于 $\overline{C}_D(\mathbf{C})$ 的 $\mathbf{C}$ 的格 (参看脚注 8), 前面所说的是 $i\Lambda=\Lambda$. 称一条定义在 $\mathbf{C}$ 的一个子域上的椭圆曲线 E 具有复乘是指, 对 $\mathbf{C}$ 中对应于此曲线的格 Λ, 存在 $\tau\in\mathbf{C}-\mathbf{R}$ 使得 $\tau\Lambda\subset\Lambda$(因此 C_D 属于这种情形, 这时 $\tau=i$); 一个这样的 τ 因此是一个系数在 $\mathbf{Z}$ 中的 2 次首 1 多项式的根.

[17] 这个公式的证明花了 100 多页 ······

均秩 $\leqslant 0.98$ (它是当 $M \longrightarrow +\infty$ 时椭圆曲线 $y^2 = x^3 + Ax + B, \sup(B^2, A^3) \leqslant M$ 的秩的平均值).

5. 滕内尔 (Tunnell) 的策略

前面提及的科兹–怀尔斯定理给出了一个判别 D 不是同余数的方法: 只需 $L(C_D, 1) \neq 1$ 即可. 反之, 如果 BSD 猜想为真 (甚至是它的弱形式), 则 $L(C_D, 1)$ 取零蕴含了 D 是同余的. 这便是滕内尔定理的证明的着手点. 因此, 问题在于计算 $L(C_D, 1)$ 从而决定这个数是否为 0. 这提出了两个严重的问题: 定义了 $L(C_D, 1)$ 的乘 [512] 积收敛得非常慢 (如果它收敛的话, 参看脚注 14), 而我们却要利用它去计算 $L(C_D, 1)$, 另外, 我们无论如何也不可能以近似状态去证明一个实数为 0, 除非额外知道它是一个整数. 滕内尔解决这两个问题的方法特别简洁.

以 $\mathscr{H} = \{z \in \mathbf{C}, \mathrm{Im}(z) > 0\}$ 记庞加莱半平面. 令 $q = e^{2i\pi z}$, 并定义 $\Theta : \mathscr{H} \to \mathbf{C}$ 为

$$\Theta(z) = \sum_{n \in \mathbf{Z}} q^{n^2}.$$

以下是滕内尔所证明的结果.

定理 F.1.12. — (Tunnell) 设 $\Omega = \int_1^{+\infty} \frac{dx}{\sqrt{x^3 - x}}$, 并令 $\sum_{n=0}^{+\infty} b_n q^n$ 为

$$\Theta(z) \cdot \Theta(2z) \cdot (2\Theta(32z) - \Theta(8z))$$

的展开式, 如果 D 是一个无平凡因子的奇数 (对于偶数也有一个类似的公式), 则有

$$L(C_D, 1) = \frac{\Omega}{16\sqrt{D}} \cdot b_D^2.$$

由于 b_D 是出现在定理 F.1.5 的条件 $(*)$ 中的那两个项的差, 那么这便解释了所谈及的定理如何能从科兹–怀尔斯定理中推出. 定理 F.1.12 的证明基于我们在下一小节要讨论的模形式的理论.

6. 模形式

如果 f 是 $\mathscr{H}$ 上的全纯函数并满足 $f(z+1) = f(z)$, 则 f 有傅里叶展开式 (q 展开式, 参看习题 VI.3.4):

$$f(z) = \sum_{n \in \mathbf{Z}} a_n q^n, \quad \text{其中 } q = e^{2i\pi z}.$$

称 f 在无限远是慢增长的是说对于 $n < 0$ 有 $a_n = 0$ 且存在 $C \in \mathbf{R}$ 使得 $a_n = O(n^C)$.

如果 N 是个整数, 以 $\Gamma_0(N)$ 代表 $\mathbf{SL}_2(\mathbf{Z})$ 的一个子群, 它由 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (其中 c 被 N 整除) 的矩阵组成. 记 $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

定义 F.1.13. — 如果 $k \in \frac{1}{2}\mathbf{N}$, 而 $j : \Gamma_0(N) \to \{\text{单位根}\}$ 满足 $j(T) = 1$, 权 k 而 j 型的模形式的空间 $M_k(\Gamma_0(N), j)$ 是 $\mathscr{H}$ 上的一个全纯函数 f 的空间, 它们满足

$$f(\frac{az+b}{cz+d}) = j\begin{pmatrix} a & b \\ c & d \end{pmatrix}(cz+d)^k f(z), \text{其中 } z \in \mathscr{H} \text{ 任意, 而 } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

并且它在无限远是慢增长的.

[513] **注记 F.1.14.** — (i) 还不完全清楚这样的形式的存在性; 事实上, 必须正确地选取函数 j 使得 $M_k(\Gamma_0(N), j)$ 非零.

(ii) $M_k(\Gamma_0(N), j)$ 是一个维数 $\leqslant 1 + \frac{Nk}{12}\prod_{p|N}(1+\frac{1}{p})$ 的有限维向量空间.

(iii) 模形式是突出的, 无所不在的. 我们在数论中, 在组合论或者在理论物理中与它们邂逅, 尽管它们是由纯解析方式定义的.

为了能感受对 $\mathbf{SL}_2(\mathbf{Z})$ 的模形式理论, 建议读者参看第 VII 章的习题 VII.6.1—VII.6.11.

- 函数 $\theta(z) = \Theta(\frac{z}{2})$ 在习题 VII.6.6 已有讨论, 这个习题的结果证明 Θ 是对 $\Gamma_0(4)$ 的权为 $\frac{1}{2}$ 的模形式, 而 j 则有点复杂.
- 如果 k 是个 $\geqslant 3$ 的偶整数, 艾森斯坦级数 $G_k(z) = \frac{(k-1)!}{2(2i\pi)^k}\sum'_{m,n}\frac{1}{(mz+n)^k}$ 是习题 VII.6.4 和 VII.6.5 的对象; 它属于 $M_k(\mathbf{SL}_2(\mathbf{Z}), 1)$, 而它的 q-展开式由 $G_k = \frac{(k-1)!\zeta(k)}{(2i\pi)^k} + \sum_{n=1}^{+\infty}\sigma_{k-1}(n)q^n$ 给出, 其中 $\sigma_t(n) = \sum_{d|n, d\geqslant 1} d^t$, 而 $t \in \mathbf{C}, n \in \mathbf{N} - \{0\}$.
- 函数 $G_2 = \frac{\zeta(2)}{(2i\pi)^2} + \sum_{n=1}^{+\infty}\sigma_1(n)q^n$ 在习题 VII.6.7 有所讨论. 它不是模形式但几乎是: $4G_2(4z) - G_2(z)$ 是模形式.

我们还要提及为滕内尔定理做了预热准备的雅可比恒等式 (1829)(参看习题 VII.6.9): $4G_2(4z) - G_2(z) = \frac{3\zeta(2)}{(2i\pi)^2}\Theta^4$, 它的证明是由观察到等式两端都属于 2 维的 $M_2(\Gamma_0(4), 1)$ 并且这个差被 q^2 整除这些事实而得到的. 比较 q-展开式便由此得到拉格朗日的 4 平方定理 (1770) 的有效形式:

$$|\{(a,b,c,d) \in \mathbf{Z}^4, a^2+b^2+c^2+d^2 = n\}| = 8\sum_{d|n, 4\nmid d} d.$$

7. 椭圆曲线和模形式

定理 F.1.15. — 如果 E 是一条定义在 $\mathbf{Q}$ 上的椭圆曲线, 而 $L(E,s) = \sum_{n=1}^{+\infty} a_n n^{-s}$, 则 $f = \sum_{n=1}^{+\infty} a_n q^n \in M_2(N_E, 1)$, 其中 N_E 是只依赖于 "坏" p 的有明确表示的一个整数.

换句话说, 一条定义在 $\mathbf{Q}$ 上的椭圆曲线是模形式的[47]. 这个结果在 1956 年由谷山丰给出了一个形式较为模糊的猜想, 而韦伊则随刚提到的志村五郎的工作之后于

[47]即 $L(E,s)$ 是一个模形式.

1966 年给出了准确的形式; 此猜想由怀尔斯[18] (在一个特殊情形中) 和 Breuil-Conrad-Diamond-Taylor 证明. $L(E,s)$ 的解析延拓性则利用了以下公式得到 (参看习题 VII. 6.3): [514]

$$L(E,s)=\frac{(2\pi)^s}{\Gamma(s)}\int_0^{+\infty}f(iy)y^s\frac{dy}{y},$$

它让我们可利用 f 的解析性质去研究 $L(E,s)$. 这是朗兰兹 (Langlands) 对于算术 L 函数的哲学 (它应该来自作为模形式推广的自守形式, 从而具有一堆漂亮的性质) 的一个特殊情形. 在曲线 C_D 的情形, 我们得到的模形式是一些 θ 函数的线性组合.

一条有模形式的椭圆曲线 E 可借助于庞加莱半平面给予它一个解析的描述. 这是构造西格勒尔点的基础 (它们是一个有理系数的二次方程的解 $\tau\in\mathscr{H}$ 的像[19]), 西格勒尔点, 正如我们提到过的, 在科里瓦金结果 (即如果 $r_\infty(E)\leqslant 1$, 则 $r(E)=r_\infty(E)$) 的证明中起了关键的作用: 这个结果自 Wiles 和 Breuil-Conrad-Diamond-Taylor 的工作以后便成为对 $\mathbf{Q}$ 上的所有椭圆曲线都成立了.

椭圆曲线具有模形式的性质的另一个应用是如下结果, 它在一个数值计算之后可以决定出 $L(E,1)$ 的值, 而在承认 BSD 猜想 (弱形式) 条件下则可提供出一个算法以决定对方程 $y^2=P(x),\deg P=3$ 的有理数解的存在性.

推论 F.1.16. — (马宁–德林费尔德 (Manin-Drinfeld), 1973) *如果 E 的方程为 $y^2=P(x)$, 且若 α 是 P 的最大实根, 则*

$$\left(\int_\alpha^{+\infty}\frac{dx}{\sqrt{P(x)}}\right)^{-1}L(E,1)$$

是一个有显式表达分母的有理数.

定理 F.1.12 证明的起始点是 Waldspurger 的一个定理 (1979). 如果 $f=\sum_{n=1}^{+\infty}a_nq^n\in M_{2k}(\Gamma_0(N),1)$, 其中 k 为整数, 又如果 D 无平方因子并与 N 互素, 且若 χ_D 是勒让德特征标 (参看脚注 13), 我们则可以证明, 定义为 $f\otimes\chi_D=\sum\chi_D(n)a_nq^n$ 的 $f\otimes\chi_D$ 是 $M_{2k}(\Gamma_0(ND^2),1)$ 中的元. Waldspurger 的定理以含糊的方式说, 这些 $L(f\otimes\chi_D,k)$ 当 D 变化时是权为 $k+\frac{1}{2}$ 而 $\Gamma_0(N')$ 的 N' 有显式表达的模形式的傅里叶系数的平方. "它不再要求" 显示这些模形式的空间的基, 并且为了得到对于所有 D 都成立的恒等式, 还计算了一些系数.

---

[18] 如果 $a^p+b^p=c^p$ 是费马大定理的一个反例, 则可考虑由 Hellegouarch 和 Frey 引进的方程 $y^2=x(x-a^p)(x+b^p)$. 怀尔斯证明了这条曲线是模形式的, 这与 Ribet(1988) 证明了的塞尔 (1984) 的一个 "ε 猜想" 相矛盾. "ε 猜想" 描述了在模形式之间我们所期待的那些同余关系. 在我们感兴趣的情形中, 这个猜想预测到在与椭圆曲线 $y^2=x(x-a^p)(y+b^p)$ 相关的模形式的 q-展开式和 $g\in M_2(\Gamma_0(2),1)$ 的模形式的 q-展开式之间的一个同余关系, 但这是不可能的, 因为这个空间是 1 维的, 并且 g 的 q-展开式的常数项被 p 整除的性质必定使这个 q-展开式的每一项均如此.

[19] 复乘理论 (脚注 16) 可以用来确定这些点的定义域; 按照 Schneider(1937) 的一个定理, 它们是 $\mathscr{H}$ 中仅有的在 $\mathbf{Q}$ 上代数的元, 并给出了 E 的代数点.

[515] F.2. 丢番图方程

1. 综述

1.1. 例子

习惯上, 一个丢番图方程是一个具有整系数的 (一个或多个变量的) 多项式方程 P(诸如, $X^2=2, DY^2=X^3-X, X^n+Y^n=Z^n, X^2+Y^2+Z^2=8n+7$, 等等), 我们感兴趣的是整数解的集合 $V_P(\mathbf{Z})$ 或是有理数解的集合 $V_P(\mathbf{Q})$. 更一般地, 可以考虑系数在一个环 A 或对于每个 A-代数 B 中的多项式方程 (后者或说成是具有从 A 到 B 的一个环态射的环 B), 而感兴趣的是在 B 的解的集合 $V_P(B)$[(20)].

解丢番图方程 P 要求描述集合 $V_P(\mathbf{Z})$ 或者 $V_P(\mathbf{Q})$, 但是可以更谨慎地问, 是否能确定 $V_P(\mathbf{Z})$ 或 $V_P(\mathbf{Q})$ 非空. 一般说来这是些非常难的问题, 它们在数学的发展中起了重大的作用.

- 希腊人因发现当多项式方程 P 为 $X^2=2$ 有 $V_P(\mathbf{Q})=\emptyset$ (无理数解 $\sqrt{2}$) 而受到了强烈的精神创伤.
- 对于方程 $X^2-DY^2=1$ (佩尔–费马) 的研究或者作为 n 函数的 P 是方程 $X^2+DY^2=n$ 对于 $V_P(\mathbf{Z})$ 的基数的研究, 再或者更一般地, 对方程 $a_1X_1^2+\cdots+a_dX_d^2=n$ 的研究产生了数的代数理论, 并且产生了二次型或连分式的理论, 还对模形式理论的发展做出了极大的贡献.
- 对方程 $X^n+Y^n=Z^n$ 已经花费了许多的笔墨, 并且在 350 多年来已产生出大量的数学理论.
- 受到费马的影响, 欧拉猜测 (1769), $X^4+Y^4+Z^4=1$ 除了显然的 $(\pm1,0,0),(0,\pm1,0),(0,$ 外没有有理数解, 这被 Elkies(1988) 所否定, 他找到了 (在计算机帮助下) 关系式 $26824404^4+153656394^4+187967604^4=206156734^4$, 并利用它证明了该方程的有理点在实点中稠密 (很难有比猜想的错误更多的了 $\cdots\cdots$).

1.2. 希尔伯特第十问题

事实上, 解丢番图方程的问题比起上面那些例子所思考的更具有基础性. 这点已被希尔伯特所了解, 在他为 1900 年的国际数学家大会准备的 23 个问题中 (第十个) 提出要找到确定丢番图方程是否有整数解的算法.

- 极容易造出一个在单变量时的算法 (我们把解决问题的愉悦留给读者).
- [516] 两个变量的这种算法的存在性已由贝克 (Baker, 1969) 证明, 这为他赢得了 1970 年度的菲尔兹奖. 它给予了贝克的是一个解的大小的一个界, 因而这个算法在于探索了到这个界前的所有可能性.
- 这个问题最后由马蒂亚塞维奇 (Matiyasevich) 在 1970 年解决, 他证明了不存在

[(20)] 例如, 如果 P 是方程 $X^2+Y^2+Z^2=8n+7$, 用手算可知 $V_P(\mathbf{Z}/8\mathbf{Z})=\emptyset$, $\mathbf{Z}/8\mathbf{Z}$ 的平方为 $0,1,4$; 这便证明了 P 没有整数解.

一个这样的算法, 这对于带着消极看法的算术学家们相信计算机将会使他们失业. 将马蒂亚塞维奇的方法向前推进, 我们实际上可以把所有数学问题以纯粹算法的方式转化为了解某个特定的丢番图方程是否有解的问题 (希尔伯特的方案并没有使算术学家们失业 ……). 我们也可以构造能随意确定是否存在整数解的显式多项式, 而不会在数学中添加矛盾 ……. 但这也有一点烦恼, 因为这意味着我们永远不可能确信我们正在着手的问题是不是这种类型.

- 马蒂亚塞维奇的定理没有排除存在能确定一个多项式 (多变量的) 是否有有理数解的算法[21], 它也没有排除对于 3 个变量的丢番图方程存在这样一个算法. 椭圆曲线构成了在这个方向上的第一个非平凡的测试, BSD 猜想如果为真便提供了一个这样的算法 (推论 F.1.16).

1.3. 方程 $Y^2 - Y = X^5 - X$

由 $Y^2 - Y = X^5 - X$ 给出的丢番图方程提供了取得进展的一个好的信号.

- 鉴于西格尔 (Siegel) 关于椭圆曲线的整点的结果, 自 1929 年以来我们便知道 $V_P(\mathbf{Z})$ 是个有限集.
- 上面提及的贝克的结果让我们能够证明: 如果 $(X,Y) \in V_P(\mathbf{Z})$, 则 $\sup(|X|,|Y|) \leqslant \exp(\exp(\exp 5^{1250}))$; 贝克的 "算法" 因此在实践中不是很有用.
- 鉴于法尔廷斯 (Faltings) 证明莫德尔猜想的结果 (参看下一小节), 自 1983 年以来我们便知道 $V_P(\mathbf{Q})$ 是个有限集.
- 计算机威力的增大使得寻找整数解成为可能 (这要求大大地缩小贝克给出的范围并可聪明地追寻可能的解, 例如, 利用 p-adic 方法). 它的完整的结果最后由 Bugeaud, Mignotte, Silsek, Stoll 和 Tengely 在 2008 年得到: [517]

$$V_P(\mathbf{Z}) = (\{-1,0,1\} \times \{0,1\}) \cup \{(2, \frac{1 \pm 11}{2}), (3, \frac{1 \pm 31}{2}), (30, \frac{1 \pm 9859}{2})\}.$$

- 并不总能知道如何计算 $V_P(\mathbf{Q})$ ……

2. 复数解的拓扑支配了算术!

2.1. 黎曼面的亏格

如果 $P \in \mathbf{C}[X,Y]$ 非零, 方程 $P(X,Y)=0$ 在 $\mathbf{C}^2$ 中的解的集合 $V_P(\mathbf{C})$ 是一条复曲线, 由于 $\mathbf{C}$ 在 $\mathbf{R}$ 上是 2 维的, 故也可以将其看作是一个实曲面; 我们称之为黎曼面.

如果 P 是方程 $X+Y=0$, 那么, $(X,Y) \mapsto X$ 诱导了从 $V_P(\mathbf{C})$ 到 $\mathbf{C}$ 上的一个同胚 (其逆为 $z \mapsto (z,-z)$). 复平面 $\mathbf{C}$ 在添加了一个无限远点 (记为 ∞) 后被自然地

[21] 可以通过增加一个变量将描述集合 $V_P(\mathbf{Q})$ 的问题转换为描述 $V_Q(\mathbf{Z})$(这个变量是这些解的分母的最小公倍数): 例如, 对方程 $DY^2 + X^3 - X$, 令 $X = \frac{a}{c}, Y = \frac{b}{c}$, 并用 c^3 乘以整个方程便成为 $Dcb^2 = a^3 - ac^2$. 如此得到的方程是个特别好的类型: 它是齐次的, 而 (a,b,c) 是其解, 同时对所有 $n \in \mathbf{Z}$, (na,nb,nc) 都是解; 因此只需在它们的集合中考虑那些 a,b,c 之间互素的元即可.

紧化, 从而得到称之为黎曼球面的球面; 换言之 $V_P(\mathbf{C})$ 同胚于减去一点 ∞ 的球面 S: 从 ∞ 出发的中心投射给出了 $S-\{\infty\}$ 到此平面的一个同胚 (如图 2).

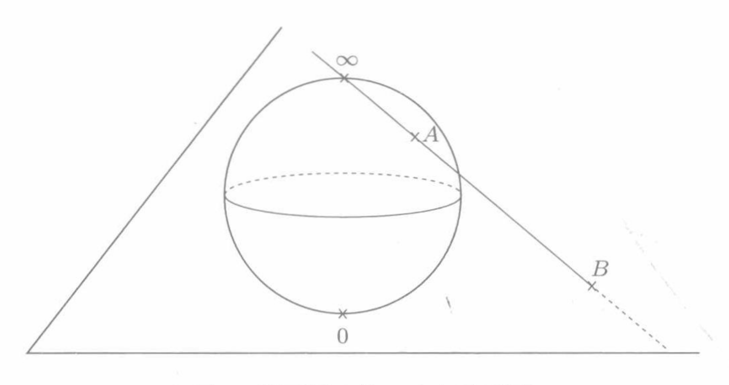


图 2. 平面是去掉一个点的球面

同样地, 如果 P 是方程 $XY=1$, 则 $(X,Y)\mapsto X$ 诱导了从 $V_P(\mathbf{C})$ 到 $\mathbf{C}^*$ 的一个同胚, 而可以将 $\mathbf{C}^*$ 看成是挖掉两个点 (0 和 ∞) 的球面.

一般地, 如果 P 是方程 $Q(X,Y)=0$, 其中 $Q\in\mathbf{C}[X,Y]$ 是不可约的 (即不能分解为形如 $Q=Q_1Q_2$, 其中 Q_1,Q_2 非常数), 于是去掉有限个奇点[22] 的 $V_P(\mathbf{C})$ 同胚 [518] 于具有有限个洞的环面, 它们对应我们去掉的有限个点. 称洞的个数为 $V_P(\mathbf{C})$ 的亏格 (记为 g)(如图 3).

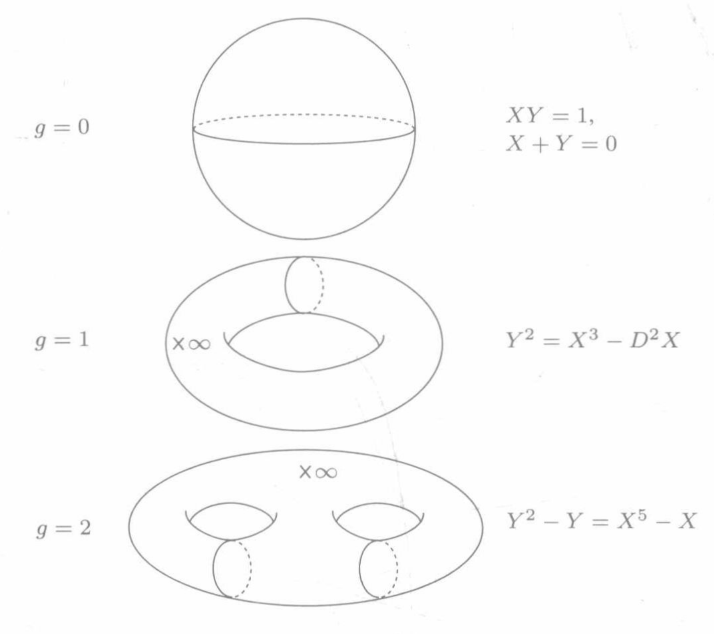


图 3. 亏格为 0, 1, 2 的黎曼面

[22] 例如, 如果 P 是方程 $Y^2=X^2(X+1)$, 则有通过 $(0,0)$ 的两个分支, 一条切于 $Y=X$, 而另一条切于 $Y=-X$. 曲面 $V_P(\mathbf{C})$ 因此是一个挖去一个点 ∞ 的球面, 并发现它的两个点在 $(0,0)$ 相互接触, 这便产生了一个奇点. 当我们去掉 $(0,0)$, 则得到挖掉 3 个点的球面 (∞ 和那两个黏合在一起的点).

- 如果 P 是 $X+Y=0$ 或 $XY=1$, 则 $g=0$.
- 如果 P 是方程 $Y^2-Y=X^5-X$, 则 $g=2$ (图 4).

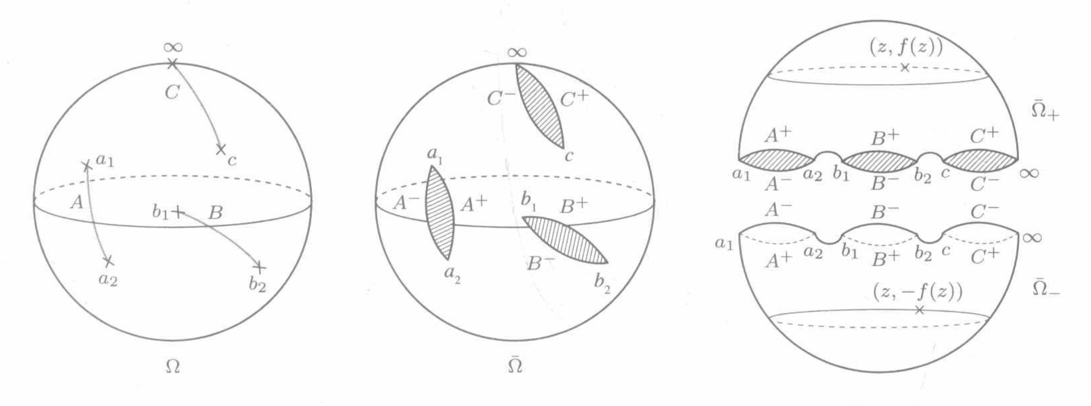


图 4. 构造函数 $\sqrt{z^5-x-\frac{1}{4}}$ 的黎曼面

「 我们来解释为什么由方程 $Y^2-Y=X^5-X$ 定义的黎曼面是一个去掉一点的具有两个洞的环面. 做变量变换 $Y=T+\frac{1}{2}$ 将其转换为 $T^2=X^5-X-\frac{1}{4}$ 而没有改变 $V_P(\mathbf{C})$ 的形状. 于是, $V_P(\mathbf{C})$ 是一对集合 $(z, \pm\sqrt{z^5-z-\frac{1}{4}}, z\in\mathbf{C})$. 对它的描述, 问题在于函数 $z\mapsto\sqrt{z^5-z-\frac{1}{4}}$ 在 $\mathbf{C}$ 上是多值的 (当我们围着多项式 $z^5-z-\frac{1}{4}$ 的零点 a_1, a_2, b_1, b_2, c 或 ∞ 中的一个绕圈子时, 这个平方根改变着符号), 因此必须注意它所产生的意义. [519]

为解决这个问题, 我们在复平面上进行切割. 在黎曼球面 $\mathbf{C}\cup\{\infty\}$ 上选取不相交的道路 A, B, C[23], 它们的端点分别是 a_1, a_2(对 A), b_1, b_2(对 B) 和 c, ∞(对 C), 并且它们不自交 (即不包含闭道), 又以 Ω 记这些道路在 $\mathbf{C}$ 中的补开集. 在 Ω 上, 多项式 $z^5-z-\frac{1}{4}$ 是一个全纯的平方根, 记为 $z\mapsto f(z)$. 另外, 如果 z 属于 A, B 或 C 并且不是 $z^5-z-\frac{1}{4}$ 的零点, 则 $f(z)$ 按照 z 沿 A"从下" 还是 "从上" 的趋向不同具有相反的极限, 即 $z^5-z-\frac{1}{4}$ 的不同的平方根. 由于考虑到这个现象, 我们将道路 A, B, C 的除了端点外的点都当作二重的, 记作 z^+ 和 z^-, 有一点像一条沿这些道路拉开的拉链. 这给了我们联结 a_1, a_2 的两条道路 A^+, A^-, 联结 b_1, b_2 的 B^+, B^- 以及联结 c 与 ∞ 的 C^+, C^-. Ω 与道路 $A^+, A^-, B^+, B^-, C^+, C^-$ 的并 $\overline{\Omega}$ 因此是一个紧集 (开的 Ω 加上了边), 而 f 被连续地延拓到 Ω(这就是这次操作的目的) 上的一个函数, 仍记作 f, 当 $z\in A, B, C$ 时它满足 $f(z^-)=-f(z^+)$(但约定在端点 z 有 $z^+=z^-=z$ 和 $f(\infty)=\infty$).

现在设 $\overline{\Omega}_+=\{(z, f(z)), z\in\overline{\Omega}\}$ 而 $\overline{\Omega}_-=\{(z, -f(z)), z\in\overline{\Omega}\}$. 那么 $\overline{\Omega}_+$ 和 $\overline{\Omega}_-$ 是 $V_P(\mathbf{C})\cup\{\infty\}$ 的两个子集, 各自同胚于 $\overline{\Omega}$ 并覆盖了 $V_P(\mathbf{C})\cup\{\infty\}$ 为了得到

[23] 让读者自己说服自己这是可能的.

$V_P(\mathbf{C}) \cup \{\infty\}$ 只要沿那些我们在构造 $\overline{\Omega}$ 时两倍了的道路粘贴起来就可以了[24]. 」

- 如果 P 是椭圆曲线的方程 $DY^2 = (X-a)(X-b)(X-c)$, 则 $g = 1$.

「用对 $Y^2 - Y = X^5 - X$ 同样的推理来论证断言的正确性: 即在黎曼球面上切开联结 a, b, c 与 ∞ 的道路. 我们还注意到变量变换 $X = 2T + \frac{a+b+c}{3}$ 和 $Y = \sqrt{\frac{2}{D}}Z$ 将此方程转换为 $Z^2 = 4T^3 - BT - C$, 且可利用问题 H.8 的结果, 按此结果 $V_P(\mathbf{C})$ 同胚于 $\mathbf{C}/\Lambda$ 减去一个点, 其中 Λ 是 $\mathbf{C}$ 的一个格. 选取 Λ 在 $\mathbf{Z}$ 上的一组基便给出了 $\mathbf{C}/\Lambda$ 到 $(\mathbf{R}/\mathbf{Z}) \times (\mathbf{R}/\mathbf{Z})$ 的同胚, 就是说到两个圆周的乘积, 这可以通过绕其中一个圆的圆心的轴旋转另一个圆实现, 从而按此方法可以得到具有一个洞的环面. 断言为真. 」

[520] • 有一个可以计算 g 的公式: 例如对于方程 $X^n + Y^n = 1$, $g = \frac{(n-1)(n-2)}{2}$. 一般的公式涉及曲线的奇点 (费马曲线没有奇点, 表明是个简单的特殊情形).

2.2. *亏格和有理数解*

解的性态按照亏格为 0,1 和 $\geqslant 2$ 有极大的差异.

- 如果 $g = 0$ 且 $V_P(\mathbf{Q})$ 至少有一个非奇点, 则存在 $C \geqslant 0$ 和 $t > 0$ 使得

$$|\{a, b, c \in \mathbf{Z}, c \geqslant 1, \sup(|a|, |b|, |c|) \leqslant x, (a, b, c) = 1, Q(\frac{a}{c}, \frac{b}{c})\}| \sim Cx^t.$$

因此, 如果至少有一个 (非奇点的) 有理数解, 则有无限多个.

- 如果 $g = 1$, 则存在 $C \geqslant 0$ 和 $r \in \mathbf{N}$ 使得

$$|\{a, b, c \in \mathbf{Z}, c \geqslant 1, \sup(|a|, |b|, |c|) \leqslant x, (a, b, c) = 1, Q(\frac{a}{c}, \frac{b}{c})\}| \sim C(\log x)^{r/2}.$$

特别地, 如果 $r \geqslant 1$, 则有无限多个有理数解, 但是这些是相当稀疏的. 一条椭圆曲线的亏格为 1, 而上面的 r 不外乎就是椭圆曲线的秩 (参看定理 F.1.6)

- 如果 $g \geqslant 2$, 则 $V_P(\mathbf{Q})$ 有限. 这是莫德尔 (1922) 的猜想, 而最终由法尔廷斯 (1983) 证明, 并为他赢得了 1986 年度的菲尔兹奖.

---

[24] 如果 $z \in A, B, C$ 不是端点, 两个点 $(z \pm \sqrt{z^5 - z - \frac{1}{4}})$ 出现在 $\overline{\Omega}_+$ 和 $\overline{\Omega}_-$ 各一次. 为了得到 $V_P(\mathbf{C}) \cup \{\infty\}$, 因此应该黏合 $\overline{\Omega}_+$ 和 $\overline{\Omega}_-$ 使得点 $(z^+, f(z^+)) \in \overline{\Omega}_+$ 与点 $(z^-, f(z^+)) \in \overline{\Omega}_-$ 黏合, 点 $(z^-, -f(z^+)) \in \overline{\Omega}_+$ 与点 $(z^+, -f(z^+)) \in \overline{\Omega}_-$ 黏合 (我们在 $\overline{\Omega}_+$ 上将 A^+, B^+, C^+ 与 $\overline{\Omega}_-$ 上的 A^-, B^-, C^- 黏合, 将 $\overline{\Omega}_+$ 上的 $\mathbf{A}^-, B^-, C^-$ 与 $\overline{\Omega}_-$ 上的 A^+, B^+, C^+ 黏合; 为了做到这一点, 应该在图上, 通过相对水平轴的旋转而非相对于水平面的对称将 $\overline{\Omega}_+$ 转到 $\overline{\Omega}_-$).

附录 G. 朗兰兹纲领简介

这一章的简洁的标题包含了许多重要却少有证明[(1)] 的陈述, 它是“朗兰兹纲领的存在性导引”, 而一个真正的导引在 M2[48] 之前是难以进行的.

朗兰兹纲领的主旨可以追溯到由欧拉做出猜测 (1783) 而由高斯证明 (1801) 的二次互反律. 这个问题是, 在给出了一个素数 ℓ 或更一般地, 一个不被任何素数的平方整除的整数 $d \in \mathbf{Z}$ 时, 描述那些使得 d 在 $\mathbf{F}_p$ 中为平方元的素数 p 的集合. 等价地, 它涉及确定多项式 $X^2 - d$ 在 $\mathbf{F}_p$ 中的零点个数. 令人惊讶的是, 此问题的答案只依赖 p 的 mod D 的类, 其中当 $d \equiv 1 \bmod 4$ 时 $D = d$, 而当 $d \equiv 2, 3 \bmod 4$ 时 $D = 4d$. 更准确地说, 存在导子为 D 并取值于 $\{\pm 1\}$ 的狄利克雷特征标 χ_D 使得 $X^2 - d$ 在 $\mathbf{F}_p$ 中的零点数等于 $1 + \chi_D(p)$.

从我们在这一章的兴趣看, 这个二次互反律可以在 L 函数间的一个乘性恒等关系中得到清楚的解释. 以 P_D 记当 $d \equiv 1 \bmod 4$ 时的多项式 $X^2 - X + \frac{1-d}{4}$, 而当 $d \equiv 2, 3 \bmod 4$ 时的多项式 $X^2 - d$. 在所有的情形中, 这个多项式是整系数的, 判别式为 D, 而它的根按照 $d \bmod 4$ 的同余分别为 $\frac{1 \pm \sqrt{d}}{2}$ 和 $\pm\sqrt{d}$. 以 A_D 代表环 $\mathbf{Z}[X]/(P_D)$. 由此当 $d \equiv 1 \bmod 4$ 时有 $A_D = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$, 而当 $d \equiv 2, 3 \bmod 4$ 时有 $A_D = \mathbf{Z}[\sqrt{d}]$. 定义函数 $\zeta_{A_D}(s) = \sum_{\mathfrak{n}} \frac{1}{|A_D(\mathfrak{n})|^s}$, 其中的 $\mathfrak{n}$ 遍历了 A_D 的使得 $A_D/\mathfrak{n}$ 为有限环的理想的集合[(2)]. 用代数数论的一点知识可以证明狄利克雷 $\zeta_{A_D}(s)$ 的级数在 $\mathrm{Re}(s) > 1$ 上收敛, 而二次互反律则等价于分解 $\zeta_{A_D}(s) = \zeta(s)L(\chi_D, s)$. [522]

例如, 如果 $d = -1$(从而 $D = -4$ 而 $A_D = \mathbf{Z}[i]$), 则特征标 χ_D 由如下给出:

[(1)]除了那些在脚注中有所概述的以外, 仅有的一些证明出现在 G.2 节, 在那里我们要将第 IV 章的傅里叶变换和 VII.2 节的梅林变换推广到阿代尔群上, 这是一个乘性的类比. 像读者将要看到的, 大部分的困难集中在实数上, 而 p-adic 数的行为极像有限群.

[(2)]注意, 如果在前面的定义中以 $\mathbf{Z}$ 替代 A_D, 我们则回到了黎曼 ζ 函数.

[48]指巴黎综合理工大学二年级的数学班.

当 $n \equiv 1 \bmod 4$ 时, 则 $\chi_D(n) = 1$, 而当 $n \equiv 3 \bmod 4$ 时, 则 $\chi_D(n) = -1$. 因此得到关系式[3]

$$\frac{1}{4} \sum_{\substack{(n,m)\in\mathbf{Z}^2 \\ (n,m)\neq(0,0)}} \frac{1}{(n^2+m^2)^s} = \zeta(s)L(\chi_4, s) = \frac{1}{1-2^{-s}} \prod_{p\equiv 1 \bmod 4} \frac{1}{(1-p^{-s})^2} \prod_{p\equiv 3 \bmod 4} \frac{1}{1-p^{-2s}},$$

将两端以 p^{-s} 表示的项相等便重新得到了费马的结果: 一个奇素数是两个平方数之和当且仅当它是形如 $4n+1$ 的数.

ζ_{A_D} 的定义可以推广到所有的环 $A = \mathbf{Z}[X_1, \ldots, X_d]/(P_1, \ldots, P_r)$, 其中 $P_1, \ldots, P_r$ 是系数在 $\mathbf{Z}$ 中的 $X_1, \ldots, X_d$ 的多项式, 可以赋予这样一个环像上面那样的一个哈塞 – 韦伊 ζ 函数 $\zeta_A(s) = \sum_{\mathrm{n}} \frac{1}{|A/\mathrm{n}|^s}$. 由于一个基数为 n 的有限环可以以唯一的方式写成基数为 $p^{v_p(n)}$ 的环的乘积 (中国剩余定理), 故函数 $\zeta_A(s)$ 有一个欧拉因子的乘积分解 $\zeta_A(s) = \prod_{p\in\mathscr{P}} \zeta_{A,p}(s)$, 而韦伊在 1949 年则提出一个猜想说 $\zeta_{A,p}(s)$ 是一个 p^{-s} 的有理函数, 这个猜想被 B. Dwork 在 1959 年证明. 韦伊也曾猜想这个有理函数有一个独立于 p 的形式的分解, 并且它只与 $P_1(z_1, \ldots, z_d) = \cdots = P_r(z_1, \ldots, z_d)$ 在 $\mathbf{C}^d$ 中的解空间有关, 它是作为格罗滕迪克对代数几何进行彻底革命化的宏伟计划的一个结果得到了证明的[4]. 分解为欧拉因子对应于函数 ζ_A 分解为 L 函数, 而朗兰兹纲领的主要目的之一是要理解这些 L 函数, 以便 (特别地) 证明哈塞 – 韦伊猜想, 即哈塞 – 韦伊函数具有到整个复平面的亚纯延拓.

最著名的例子大概要数 $A = \mathbf{Z}[X, Y]/(Y^2 - X^3 - \alpha X^2 - \beta X - \gamma)(\alpha, \beta, \gamma \in \mathbf{Z})$ 的情形了. 在此情形, 怀尔斯 (1994, 在所谓的 "半稳定" 情形下) 以及 C. Breuil, B. Conrad, F. Diamond 和 R. Taylor (1999, 在一般情形下) 证明了这个已由谷山丰在 1956 年模糊地提出而韦伊在 1966 年准确提出的猜想, 它说的是, 存在一个本原的模形式 f (参看 G.1 的 4.1 小节) 使得 $\zeta_A(s) = \frac{\zeta(s-1)}{L(f,s)}$, 但可以相差有限多个无害的欧拉 [523] 因子的乘积. 这让怀尔斯在利用 K. Ribet (1988) 前面的结果后能够推导出不存在前面那样形式的 A 使得 $X^3 + \alpha X^2 + \beta X + \gamma = X(X - a^p)(X + b^p)$, 其中 $a^p + b^p = c^p$ 是费马大定理的一个反例, 因此他证明了费马大定理.

G.1. 阿廷 (Artin) 猜想

1. 群 $\mathscr{G}_{\mathbf{Q}}$

回顾一下 (参看小词典的 8.2 和 8.3). $x \in \mathbf{C}$ 是代数的是指存在非零的 $P \in \mathbf{Q}[X]$, 使得 $P(x) = 0$. 等价地, $x \in \mathbf{C}$ 是代数的当且仅当 $\mathbf{C}$ 的由 x 生成的 $\mathbf{Q}$-子代数 $\mathbf{Q}[x]$

---

[3] $\mathbf{Z}[i]$ 是主理想环, 于是如果 $n + im \in \mathbf{Z}[i]$ 非零, 则 $\mathbf{Z}[i]/(n + im)$ 有限, 其基数为 $n^2 + m^2$; 因子 $\frac{1}{4}$ 可解释为: 当 $\alpha = n + im \in \mathbf{Z}[i] - \{0\}$ 时, $\alpha, -\alpha, i\alpha, -i\alpha$ 生成同一个理想.

[4] 这为他赢得了 1966 年度的菲尔兹奖; 德利涅 (P. Deligne) 则由于证明了韦伊猜想的最后一个, 即有限域上的黎曼猜想, 得到了 1978 年度的菲尔兹奖, 这个猜想说的是 $\zeta_{A,p}(s)$ 的零点和极点分布在有限条显式表示的竖直直线上.

在 $\mathbf{Q}$ 上的维数有限; 因此, 这是个子域. 因此可以证明, 如果 x, y 为代数的, 则 $x+y$ 和 xy 也都是代数的. 于是代数数的集合 $\overline{\mathbf{Q}}$ 是 $\mathbf{C}$ 的一个子域.

以 $\mathscr{G}_{\mathbf{Q}}$ 记 $\overline{\mathbf{Q}}$ 的域自同构的集合, 就是说, $\overline{\mathbf{Q}}$ 那些置换 σ 的集合, 它们满足

$$\sigma(x+y)=\sigma(x)+\sigma(y) \quad 和 \quad \sigma(xy)=\sigma(x)\sigma(y), \quad 其中\ x,y\in\overline{\mathbf{Q}}.$$

在复合下, $\mathscr{G}_{\mathbf{Q}}$ 是 $\overline{\mathbf{Q}}$ 的置换群的子群; 这甚至是 $\overline{\mathbf{Q}}$ 的 $\mathbf{Q}$-线性自同构群的子群[5].

$\mathscr{G}_{\mathbf{Q}}$ 是个非常巨大且极端神秘的群, 但对它的了解对于许多问题是关键的. 单就它的存在性这样简单的事实已经非常有用了.

- 在 $\mathscr{G}_{\mathbf{Q}}$ 中我们知道如何描述的唯一的元是复共轭, 我们将其记为 frob_∞. 我们有 $(\mathrm{frob}_\infty)^2=1$, 而阿廷 (1924) 证明了 $\mathscr{G}_{\mathbf{Q}}$ 中的每个有限阶的元共轭于 1 或者 frob_∞, 因此阶为 1 或 2.
- 如果 $P\in\mathbf{Q}[X]$ 为 n 次不可约多项式, 且若 $\alpha_1,\ldots,\alpha_n\in\overline{\mathbf{Q}}$ 为 P 的根, 则对任意的 $i,j\in\{1,\ldots,n\}$, 存在 $\sigma_{i,j}\in\mathscr{G}_{\mathbf{Q}}$ 满足 $\sigma_{i,j}(\alpha_i)=\alpha_j$[6], 这证明了在 $\mathscr{G}_{\mathbf{Q}}$ 中除了 frob_∞ 外还有其他的元.
- 如果 H 是 $\mathscr{G}_{\mathbf{Q}}$ 的一个子群, 则 $\overline{\mathbf{Q}}$ 中在 H 作用下的不动元的集合 $\overline{\mathbf{Q}}^H$ 是 $\overline{\mathbf{Q}}$ 的一个子域. 反之, 如果 K 是 $\overline{\mathbf{Q}}$ 的一个子域, 使得 K 中每个元不动的 $\sigma\in\mathscr{G}_{\mathbf{Q}}$ 的集合 $\mathscr{G}_K$ 是 $\mathscr{G}_{\mathbf{Q}}$ 的一个闭子群[7]. 于是按这种方式[8] 得到了这些数域 (即 $\overline{\mathbf{Q}}$ 中在 $\mathbf{Q}$ 上的有限维 [524] 的子域) 与 $\mathscr{G}_{\mathbf{Q}}$ 的具有有限指标的闭子群[9] 之间的一个双射, 于是, 当 K 是个数域时有 $\overline{\mathbf{Q}}^{\mathscr{G}_K}=K$, 而当 H 是 $\mathscr{G}_{\mathbf{Q}}$ 的一个具有有限指标的闭子群时有 $\mathscr{G}_{\overline{\mathbf{Q}}^H}=H$.
- 有猜想说 $\mathscr{G}_{\mathbf{Q}}$ 是如此复杂以致所有的有限群 G 都是 $\mathscr{G}_{\mathbf{Q}}$ 的商[10] (伽罗瓦逆问题). 我们已知如何证明它对于以下情形为真[11]：所有奇数阶的群 (沙法列维奇,1954), 对任意 n 的 S_n 和 A_n, 对于大魔群 ……; 例如我不认为已经知道了对 $\mathbf{SL}_3(\mathbf{F}_9)$($\mathbf{F}_9$ 是 9 个元组成的域) 的证明, 尽管它比大魔群要小得多.

---

[5] 可以先证明 $\sigma(1)=1$, 然后对任意的 $n\in\mathbf{Z}$ 得到 $\sigma(n)=n$, 而最后证明 σ 在 $\mathbf{Q}$ 上为恒等.

[6] 这是伽罗瓦理论的一个结果.

[7] 在 $\mathscr{G}_{\mathbf{Q}}$ 上取克鲁尔 (Krull) 拓扑, 按定义, 当 $\overline{\mathbf{Q}}$ 为离散拓扑时, 它是使 $\mathscr{G}_{\mathbf{Q}}$ 的作用为连续的最弱的拓扑. 这意味着, 如果 $\sigma_0\in\mathscr{G}_{\mathbf{Q}}$ 而 $\alpha\in\overline{\mathbf{Q}}$, 集合 $U_\alpha(\sigma_0)=\{\sigma\in\mathscr{G}_{\mathbf{Q}},\sigma(\alpha)=\sigma_0(\alpha)\}$ 是 $\mathscr{G}_{\mathbf{Q}}$ 的一个开集, 且这些 $U_\alpha(\sigma_0):\sigma_0\in\mathscr{G}_{\mathbf{Q}}(\alpha\in\overline{\mathbf{Q}})$ 构成 $\mathscr{G}_{\mathbf{Q}}$ 的开集基. 特别地, $\mathscr{G}_{\mathbf{Q}}$ 的所有包含 1 的开集都包含了对于某个 $\alpha\in\overline{\mathbf{Q}}$ 的 $U_\alpha(1)$, 从而包含了一个有限指数的子群.

[8] 这又是伽罗瓦理论的一个结果.

[9] 回想一下: 如果 $H\subset G$ 为群, H 在 G 中的指标 $[G:H]$ 是 G/H 的基数.

[10] 如果此为真, 那么 $G\times\cdots\times G$ 也是 $\mathscr{G}_{\mathbf{Q}}$ 的商, 从而 G 以无限多种不同的方式成为 $\mathscr{G}_{\mathbf{Q}}$ 的商.

[11] 为了证明这种类型的断言, 我们可以按照以下的方式进行. 如果 $P\in\mathbf{Q}[X]$ 而 $\alpha\in\overline{\mathbf{Q}}$ 满足 $P(\alpha)=0$, 并且若 $\sigma\in\mathscr{G}_{\mathbf{Q}}$, 则 $0=\sigma(P(\alpha))=P(\sigma(\alpha))$(因为 α 使得系数不动). 我们便如此得到了一个从 $\mathscr{G}_{\mathbf{Q}}$ 到 P 的根的置换群的群态射. 对它的像 Gal_P 的描述 (由构造知它是 $\mathscr{G}_{\mathbf{Q}}$ 的商) 是伽罗瓦理论的研究对象. 如果 P 是 n 次不可约的, 则 Gal_P 是 S_n 的一个子群, 一般来说等于 S_n; 对于构造一个不可约多项式 P 使得 Gal_P 不是个对称群而言, 这必定是个不好的技巧. 例如, 构造一个多项式 P 使得 Gal_P 是大魔群则用了复几何、代数拓扑、有限群论、代数几何和数论的混合知识.

2. $\mathscr{G}_{\mathbf{Q}}$ 的表示

在第 I 章我们已提到过要在 $\mathscr{G}_{\mathbf{Q}}$ 上通过它的表示来了解它. 我们只对复表示感兴趣; 它起着基础性的作用, 但由于拓扑的关系[12] 对于许多应用有点过于刚性, 它也会被引导去考虑 $\mathscr{G}_{\mathbf{Q}}$ 在其他不同于 $\mathbf{C}$ 的域 (甚至环) 上的表示, 譬如 p-adic 数的域 $\mathbf{Q}_p$. 如在脚注 12 中解释的那样, 如果 V 是 $\mathscr{G}_{\mathbf{Q}}$ 的一个复表示, 那么 $\mathscr{G}_{\mathbf{Q}}$ 通过有限群作用, 让我们可以利用第 I 章的结果. 另外, 为了解释出现在第 3 节的阿廷猜想中的那些对 [525] 象而所有必要的计算都是在被 ρ_V 的核固定不动的数域 K 中进行的. 这解释了为什么尽管我们没有掌握全部的 $\mathscr{G}_{\mathbf{Q}}$, 这些还是可行的.

如果 $P \in \mathbf{Q}[X]$, 则 $\mathscr{G}_{\mathbf{Q}}$ 交换 P 的根, 故给了 $\mathscr{G}_{\mathbf{Q}}$ 一个置换表示 V_P. 可以证明 $\mathscr{G}_{\mathbf{Q}}$ 的所有不可约表示都可作为一个 V_P 表示的分支出现, 但是试图通过列出 $\mathbf{Q}[X]$ 的所有元素 P 并分解这些 V_P 为不可约分支来了解 $\mathscr{G}_{\mathbf{Q}}$ 的效率有点像希望将黎曼假设的证明落在列出所有的逻辑命题上一样. 但仍旧有可以由这种方式得到的 $\mathscr{G}_{\mathbf{Q}}$ 的表示的两个例子.

- 平方根. 如果 $d \in \mathbf{Q}^*$ 不是 $\mathbf{Q}$ 中的一个平方数, 则 $\sqrt{d} \notin \mathbf{Q}$, 而如果 $\sigma \in \mathscr{G}_{\mathbf{Q}}$, 则存在 $\eta_d(\sigma) \in \{\pm 1\}$ 使得 $\sigma(\sqrt{d}) = \eta_d(\sigma)\sqrt{d}$, 且容易证明 $\sigma \mapsto \eta_d(\sigma)$ 是 $\mathscr{G}_{\mathbf{Q}}$ 的一个线性表示.

- 单位根. 设 D 为 $\geqslant 3$ 的整数, 而 $\alpha = e^{2i\pi/D}$. 于是 $\alpha^D = 1$ 且对于 D 的所有严格的因子 d 有 $a^d \neq 1$. 现在如果 $\sigma \in \mathscr{G}_{\mathbf{Q}}$, 则 $\sigma(\alpha)^D = \sigma(\alpha^D) = 1$, 并且 $\sigma(\alpha)^d = \sigma(\alpha^d) \neq 1$, 其中 d 为 D 的严格因子, 因此存在 $\chi_{\mathrm{cycle},D}(\sigma) \in (\mathbf{Z}/D\mathbf{Z})^*$ 使得 $\sigma(\alpha) = e^{2i\pi\chi_{\mathrm{cycle},D}(\sigma)/D} = \alpha^{\chi_{\mathrm{cycle},D}(\sigma)}$. 于是有 $\sigma(\alpha^n) = \alpha^{n\chi_{\mathrm{cycle},D}(\sigma)}$, 其中 $n \in \mathbf{Z}$; 由此得到 $\chi_{\mathrm{cycle},D} : \mathscr{G}_{\mathbf{Q}} \to (\mathbf{Z}/D\mathbf{Z})^*$ 是一个群态射[13]. 它给予每个本原的狄利克雷特征标 χ 一个 $\mathscr{G}_{\mathbf{Q}}$ 的 1 维连续表示 ρ_χ: 如果 χ 是这样一个特征标, 且若 D 是其导子, 则 $\rho_\chi = \chi \circ \chi_{\mathrm{cycle},D}$ 是从 $\mathscr{G}_{\mathbf{Q}}$ 到 $\mathbf{C}^*$ 的一个群态射.

定理 G.1.1. — (克罗内克–韦伯 (Kronecher-Weber)) $\mathscr{G}_{\mathbf{Q}}$ 的所有 1 维表示均具有 ρ_χ 的形式, 其中 χ 是一个本原的狄利克雷特征标.

克罗内克发布了 (1853) 这个定理, 但直到 1886 年才有了一个 (几乎) 正确的证明 (由韦伯).

鉴于这个克罗内克–韦伯定理, 那么当考虑 $\mathscr{G}_K$ 的 1 维表示 (其中 K 为数域) 时,

---

[12] 如果 $\rho : \mathscr{G}_{\mathbf{Q}} \to \mathbf{GL}_n(\mathbf{C})$ 是群的连续态射, 则有 $\rho(1) = 1$, 且 ρ 的连续性表明 (参看脚注 7) 存在一个 $\mathscr{G}_{\mathbf{Q}}$ 的具有有限指标的子群 H 使得, 如果 $g \in H$, 则 $\rho(g) - 1$ 的所有坐标 $a_{i,j}$ 满足 $|a_{i,j}| \leqslant \frac{1}{2n}$. 将此应用到 g^k 上, 由此便得到对任意的 $k \in \mathbf{Z}$ 有 $|\mathrm{Tr}(\rho(g)^k) - n)| \leqslant \frac{1}{2}$, 而且不难由此得出结论, 这蕴含了 $\rho(g)$ 的所有特征值均等于 1, 从而 $\rho(g) = 1$. 最后得知, ρ 的核包含了一个具有有限指标的群, 从而 $\rho(\mathscr{G}_{\mathbf{Q}})$ 是个有限群. 特别地, $\mathscr{G}_{\mathbf{Q}}$ 的每个复表示只在 $\mathscr{G}_{\mathbf{Q}}$ 的一个小的部分提供了信息. 在 $\mathbf{Q}_p$ 上情况则要好得多, 在哈塞–韦伊 ζ 函数 $\zeta_A, A = \mathbf{Z}[X_1, \ldots, X_d]/(P_1, \ldots, P_r)$ 分解式中出现的 L 函数的自然定义利用了 $\mathscr{G}_{\mathbf{Q}}$ 的表示, 这是格罗滕迪克相关于方程 $P_1 = \cdots = P_r = 0$ 定义的簇得到的.

[13] 这是分圆特征标.

或者当考虑对固定 n, $\mathscr{G}_{\mathbf{Q}}$ 的 n 维表示时, 又或者我们将这两个问题混合, 并考虑 $\mathscr{G}_K$ 的 n 维表示, 其中 n 固定而 K 为数域时, 我们不知道会发生什么. 我们称对 $\mathscr{G}_K$ 的 1 维表示的描述为类域论 (在 20 世纪的头 30 年它在算术学中占了统治地位).

维数 $\geqslant 2$ 长期以来都被认为是解决无望的.

3. 阿廷 L 函数

[526]

设 $\mathscr{P}$ 是素数的集合. 如果 $p \in \mathscr{P}$, 则以 $|\ |_p$ 记 $\mathbf{Q}$ 上的 p-adic 范数, 并选取 $|\ |_p$ 在 $\overline{\mathbf{Q}}$ 上的一个扩张[14]. 然后以 $\mathscr{G}_{\mathbf{Q}_p}$ 记 $\sigma \in \mathscr{G}_{\mathbf{Q}}$ 在 $|\ |_p$ 下为等距态射的 σ 的集合. 又以 I_p 记那些对任意与 p 互素的 D 满足 $\sigma(e^{2i\pi/D}) = e^{2i\pi/D}$ 的 $\sigma \in \mathscr{G}_{\mathbf{Q}_p}$ 的子群. 称 $\mathscr{G}_{\mathbf{Q}_p}$ 中的一个元 σ 是在 p 的一个弗罗贝尼乌斯 (Frobenius) 是说 $\sigma(e^{2i\pi/D}) = e^{2i\pi p/D}$, 其中 D 为任意与 p 互素的数. 按 I_p 的定义, 两个在 p 的弗罗贝尼乌斯只相差一个 I_p 中的元. 选取在 p 的一个弗罗贝尼乌斯 frob_p.

设 V 是 $\mathscr{G}_{\mathbf{Q}}$ 的一个 n 维表示. 如果 p 是一个素数, 那么以 V^{I_p} 记被 I_p 保持不动的子空间. 可以证明[15]对几乎所有的 p [16]有 $V^{I_p} = V$. frob_p 在 V^{I_p} 上的作用不依赖 frob_p 的选取, 从而 $E_p(V,T) = \det(1 - T\rho_{V^{I_p}}(\mathrm{frob}_p))$ 既不依赖 frob_p 的选取也不依赖 $|\ |_p$ 到 $\overline{\mathbf{Q}}$ 的扩张. 这是一个 $\dim V^{I_p}$ 次的多项式, 因此 $E_p(V,T)$ 对几乎所有的 p 是一个 n 次的多项式. 定义与 V 相关的阿廷 L 函数 $L(V,s)$ 为欧拉乘积

$$L(V,s) = \prod_{p \in \mathscr{P}} E_p(V, p^{-s})^{-1}.$$

例题 G.1.2. — (i) 如果 $V = \mathbf{1}$ 是个平凡表示, 则 $V^{I_p} = V$, 从而有 $E_p(V,T) = 1 - T$, 其中 p 任意. 因此有 $L(\mathbf{1}, s) = \prod_{p \in \mathscr{P}} (1 - p^{-s})^{-1} = \zeta(s)$.

(ii) 更一般地, 如果 χ 是一个本原狄利克雷特征标, 则有 $L(\rho_\chi, s) = L(\chi, s)$.

(iii) $d \in \mathbf{Z}$ 为不被任意素数的平方整除的整数, 并设 D 和 χ_D 是取值在 $\{\pm 1\}$ 中的 $\bmod D$ 的狄利克雷特征标, 这在简介中已出现过. 简介中的二次互反律可重新写成一个在阿廷 L 函数和狄利克雷 L 函数之间的等式 $L(\eta_d, s) = L(\chi_D, s)$.

(iv) 如果 V_1 和 V_2 是 $\mathscr{G}_{\mathbf{Q}}$ 的两个表示, 而 $V = V_1 \oplus V_2$, 则 $L(V,s) = L(V_1,s)L(V_2,s)$. 例如, 表示 $V = \mathrm{Ind}_{\mathscr{G}_{\mathbf{Q}[\sqrt{d}]}}^{\mathscr{G}_{\mathbf{Q}}} \mathbf{1}$ 可分解为 $V = \mathbf{1} \oplus \eta_d$, 从而简介中的恒等式 $\zeta_{A_D}(s) = \zeta(s)L(\chi_D, s)$ 不过是恒等式 $L(V,s) = L(\mathbf{1},s)L(\eta_d,s)$ 的翻版.

一个阿廷 L 函数的次是 $\mathscr{G}_{\mathbf{Q}}$ 的这个表示空间的维数; 这也几乎是所有这些欧拉因子的次数. 根据克罗内克–韦伯定理, 这些狄利克雷 L 函数 (包括了 ζ 函数) 描述了 1 [527]

---

[14] 要构造这样一个范数只需选取从 $\overline{\mathbf{Q}}$ 到 $\mathbf{Q}$ 在 $\mathbf{Q}_p$ 中的整闭包的一个同构即可 (参看小词典的 20.4.5 小节, 同样在小词典的 8.3 和 8.8 有 $\mathbf{Q}$ 在 $\overline{\mathbf{Q}}_p$ 中的整闭包实际同构于 $\overline{\mathbf{Q}}$ 的事实). 用代数数论的技术我们可以证明, 如果我们有到 $\overline{\mathbf{Q}}$ 的两个扩张 $|\ |_{p,1}$ 和 $|\ |_{p,2}$, 则对所有的 $x \in \overline{\mathbf{Q}}$ 存在 $\sigma \in \mathscr{G}_{\mathbf{Q}}$ 使得 $|x|_{p,2} = |\sigma(x)|_{p,1}$, 这便解释了随后的结果不依赖这个扩张的选取.

[15] 这又是代数数论的一个结果.

[16] "对几乎所有的 p" 的意思是 "除去有限个 p 外".

次的阿廷 L 函数的集合. 由定理 VII.3.4 和 VII.4.4 得到了以下定理.

定理 G.1.3. — 一个 1 次的阿廷 L 函数具有到整个 $\mathbf{C}$ 的亚纯延拓, 当 $L=\zeta$ 时它在 $s=1$ 之外全纯.

猜想 G.1.4. — (阿廷, 1923) 如果 V 为维数 $\geqslant 2$ 的不可约表示, 则 $L(V,s)$ 具有到整个 $\mathbf{C}$ 的全纯延拓.

这个猜想离解决差得尚远, 但近来在维数 2 的情形有可观的进展.

用类域论可以证明 (参看定理 G.1.8 和 G.1.9), 如果 K 是数域, 且 χ 是 $\mathscr{G}_K$ 的线性特征标, 则 $L(\mathrm{Ind}_{\mathscr{G}_K}^{\mathscr{G}_\mathbf{Q}}\chi,s)$ 除了 $\chi=\mathbf{1}$ 的情形外在 $\mathbf{C}$ 上全纯, 而当 $\chi=\mathbf{1}$ 时它在单极点 $s=1$ 之外全纯.

阿廷自己利用这个结果和有限群的表示论 (更准确地说是定理 I.3.19, 它是主要动机 [17]) 证明了 $L(V,s)$ 的一个幂有到整个 $\mathbf{C}$ 的亚纯延拓. 如果利用布饶尔定理 (定理 I.3.20) 代替阿廷定理, 则可证明 (这是布饶尔的主要动机)$L(V,s)$ 有到整个 $\mathbf{C}$ 上的亚纯延拓.

朗兰兹 (R. Langlands, 1967) 提出了一个宏伟的纲领, 它的一个目标就是证明阿廷猜想.

4. 2 次 L 函数

4.1. 奇表示和模形式

设 D 为整数而 $\Gamma_0(D)$ 是形如矩阵 $\begin{pmatrix}a&b\\c&d\end{pmatrix}$ 的集合, 其中系数属于 $\mathbf{Z}$ 并满足 $ad-bc=1$ 以及 $c\equiv 0 \bmod D$. 它是 $\mathbf{SL}_2(\mathbf{Z})$ 的子群, 是 $\mathbf{SL}_2(\mathbf{Z}/D\mathbf{Z})$ 中上三角矩阵群在 $\mathbf{SL}_2(\mathbf{Z})$ 中的逆像.

如果 $k\geqslant 1$ 为整数, 并且 χ 是 $\bmod D$ 的狄利克雷特征标, 那么一个权为 k、D 级、特征标为 χ 的 [18] 拟模形式 f 是 $\mathscr{H}$ 上的一个全纯函数, 使得 $f(\frac{az+b}{cz+d})=$ [528] $\chi(d)(cz+d)^k f(z)$, 其中 $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma_0(D)$. 一个拟模形式特别是一个周期为 1 的周期

[17] 设 H 是 ρ_V 的核, 并设 $G=\mathscr{G}_\mathbf{Q}/H$; 这是一个有限群, 而 V 可以看成是 G 的一个表示. 根据定理 I. 3.19, 存在 $d_V\in\mathbf{N}$, 一个对于 $i\in I$ 的族 (C_i,χ_i,n_i) 使得 $\chi_V=\sum_{i\in I}n_i\mathrm{Ind}_{C_i}^G\chi_i$, 其中 C_i 是 G 的一个 (循环) 子群, χ_i 是 C_i 的线性特征标, 而 $n_i\in\mathbf{N}$. 那么, 设 K_i 是使得 $\mathscr{G}_{K_i}$ 是 C_i 在 $\mathscr{G}_\mathbf{Q}$ 中的逆像的数域. 我们可以将 χ_i 想成是 $\mathscr{G}_{K_i}$ 的一个线性特征标, 并从例题 G.1.2 的 (iv) 推导出关系式

$$L(V,s)^{d_V}=\prod_{i\in I}L(\mathrm{Ind}_{\mathscr{G}_{K_i}}^{\mathscr{G}_\mathbf{Q}}\chi_i,s)^{n_i}.$$

[18] 如果 $D=1$, 则有 $\Gamma_0(D)=\mathbf{SL}_2(\mathbf{Z})$ 和 $\chi=1$. 由于 $\mathbf{SL}_2(\mathbf{Z})$ 由 $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ 和 $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ 生成, 则拟模性质等价于条件 $f(z+1)=f(z)$ 和 $z^{-k}f(-1/z)=f(z)$, 这是在 VII.5 的习题中用到过的.

函数, 从而有一个如下形式的傅里叶展开 (q-展开)

$$f(z)=\sum_{n\in\mathbf{Z}}a_n(f)q^n,\ \text{其中}\ q=e^{2i\pi z}.$$

称 f 是一个权为 k、D 级、特征标为 χ 的抛物 (或尖点) 模形式, 即它是个拟模形式, 并在无限远速降, 这表明 $\operatorname{Im}(z)^N(cz+d)^{-k}f(\frac{az+b}{cz+d})$ 对于任意的 $N\in\mathbf{N}$ 和 $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathbf{SL}_2(\mathbf{Z})$ 在半平面 $\operatorname{Im}(z)\geqslant 1$ 上有界[19]. 以 $S_k(D,\chi)$ 记这些模形式的空间.

如果 $f\in S_k(D,\chi)$. 因为在无限远速降的条件, 我们特别有 $a_n(f)=0$, $n\leqslant 0$, 并像在习题 VII.6.3 那样我们可以证明 $a_n(f)=O(n^{k/2})$, 这让我们对于每个 f 配以一个 L 函数, 其定义为

$$L(f,s)=\frac{(2\pi)^s}{\Gamma(s)}\int_0^{+\infty}f(iy)y^s\frac{dy}{y}=\sum_{n=1}^{+\infty}\frac{a_n(f)}{n^s}.$$

稍加计算便能证明 $f\mapsto f_{|k}w$ 将 $S_k(D,\chi)$ 映到 $S_k(D,\overline{\chi})$, 其中 $f_{|k}w$ 的定义为 $(f_{|k}w)(z)=z^{-k}f(-1/Dz)$. 这让我们像在习题 VII.6.3, VII.6.6 中那样, 将上面的积分在 $\sqrt{D}$ 处截断, 来证明 $L(f,s)$ 有到整个 $\mathbf{C}$ 上的全纯延拓, 并满足一个联系 s 和 $k-s$ 的函数方程. 如果 f 使得 $L(f,s)$ 满足如下条件则称它为本原的:

- 有一个欧拉因子的乘积展开

$$L(f,s)=\prod_{p|D}\frac{1}{1-a_p(f)p^{-s}}\prod_{p\nmid D}\frac{1}{1-a_p(f)p^{-s}+\chi(p)p^{k-1-2s}},$$

- 有一个形如 $\Lambda(f,k-s)=w\Lambda(f^*,s)$ 的函数方程, 其中 $f^*(z)=\overline{f(-\bar{z})}$, w 是一个模为 1 的复数, 而

$$\Lambda(f,s)=\frac{\Gamma(s)}{(2\pi)^s}D^{s/2}L(f,s).$$

虽然本原模形式的存在性需要一个奇迹, 但 Atkin 和 Lehner 却证明了当 f 遍历权为 k 的模形式时, $f(\frac{az+b}{d})$(其中 $a,b,d,a\neq 0,d\neq 0$) 构成了由权为 k、级任意的抛物形式生成的向量空间的一个生成元族.

定理 G.1.5. — 如果 $\rho:\mathscr{G}_{\mathbf{Q}}\to\mathbf{GL}_2(\mathbf{C})$ 是一个奇的不可约表示[20], 则存在一个权为 1 的本原模形式 f 使得 $L(f,s)=L(\rho,s)$. 特别地, 对于这样的表示阿廷猜想为真.

这个定理是全新的; 它在 2007 年 1 月宣布, 而文章则在 2008 年 10 月完成. [529]

---

[19] 由于 $f(\frac{az+b}{cz+d})=\chi(d)(cz+d)^kf(z)$, $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma_0(D)$, 故只要证明它对于一个 $\Gamma_0(D)\backslash\mathbf{SL}_2(\mathbf{Z})$ 的一个代表系成立即可, 而这是一个有限集.

[20] 它的意思是 $\rho(\mathrm{frob}_\infty)\neq\pm 1$ 而 $\det\rho(\mathrm{frob}_\infty)=-1$, 这是迄今最常见的情形. 如果 $\det\rho(\mathrm{frob}_\infty)=1$, 则称此表示为偶的.

ρ 在 $\mathbf{PGL}_2(\mathbf{C})$ 的像的情形是个二面体群[21], 这可追溯到 30 年代, 是阿廷和赫克的工作. 朗兰兹纲领的一个最初成功是证明了在像不是 A_5 的情形中的这样的结果 (朗兰兹 (1980) 和滕内尔 (Tunnell, 1981)). 它特别覆盖了 ρ 在 $\mathbf{GL}_2(\mathbf{C})$ 中的像是群 $\mathbf{GL}_2(\mathbf{F}_3)$ 的情形[22], 它是怀尔斯证明费马大定理的出发点. 全世界的数学家们已经将怀尔斯的方法转化成一个有效的机制, 即从一个点过渡到在 $\mathscr{G}_{\mathbf{Q}}$ 的 2 维表示的集合中的一个点. 最后触及它的是 Kisin (澳大利亚人, 哈佛的博士后), Khare (印度人, 洛杉矶分校的博士后) 和 Wintenberger (斯特拉斯堡)[23]. 证明中有意思之处是, 他们通过对素数集合的归纳进行.

4.2. 一个例子

我们已经注意到, 如果 $P = X^d + \alpha_{d-1}X^{d-1} + \cdots + \alpha_0 \in \mathbf{Z}[X]$, 则 $\mathscr{G}_{\mathbf{Q}}$ 置换 P 的根; 以 V_P 记由此得到的 $\mathscr{G}_{\mathbf{Q}}$ 的置换表示. 现在, 所有的置换表示 V_P 可以分解为 $V_P = \mathbf{1} + \rho_P$, 其中 $\mathbf{1}$ 是平凡表示. 这个分解产生了分解 $L(V_P, s) = \zeta(s)L(\rho_P, s)$.

如果 p 是一个素数, 以 $N_p(P)$ 记 P 在 $\mathbf{F}_p$ 中的根的个数.

- 如果 $P = X^2+X+6$, P 的判别式于是等于 -23, 二次互反律给了我们一个狄利克雷特征标 $\chi_{23} : (\mathbf{Z}/23\mathbf{Z})^* \to \{\pm 1\}$ 使得对所有的 p 有 $N_p(P) = 1+\chi_{23}(p)$(对于 $p = 23$ 按约定有 $\chi_{23}(p) = 0$, 它在 $\mathbf{F}_{23}$ 中有一个二重根). 因此 $L(\rho_P, s) = L(\chi_{23}, s)$, 无任何神秘可言.

- 如果 $P = X^3 - X - 1$, 于是其判别式为 23 的幂, 且在 $\mathbf{F}_{23}$ 中有一个二重根. 我们有 $L(\rho_P, s) = \prod_{p\in\mathscr{P}} \frac{1}{1-(N_p(P)-1)p^{-s}+\chi_{23}(p)p^{-2s}}$($\chi_{23}$ 的出现显示了 $\mathbf{Q}(\sqrt{-23})$ 是 P 的根生成的域的一个子域). 将 $L(\rho_P, s)$ 写成一个狄利克雷级数 $\sum_{n\geqslant 1} a_n n^{-s}$ 从而对 $n \geqslant 1$ 定义了 a_n(因此当 p 为素数时 $a_p = N_p(P) - 1$, 而级数 $\sum_{n\geqslant 1} a_n n^{-s}$ 对 $P \bmod p$ 在 p 变化时的行为进行了编码). 对 $L(\rho_P, s)$ 的定理 G.1.5 给出了恒等式 [530]

$$\sum_{n\geqslant 1} a_n q^n = \frac{1}{2}\Big(\sum_{x,y\in\mathbf{Z}} q^{x^2+xy+6y^2} - \sum_{x,y\in\mathbf{Z}} q^{2x^2+xy+3y^2}\Big) = q\prod_{k\geqslant 1}(1-q^k)(1-q^{23k}).$$

对这些恒等式中第一个的证明可借助于类域论将 ρ_P 写成由 $\mathscr{G}_{\mathbf{Q}(\sqrt{-23})}$ 的一个线性特征标诱导的形式而得到. 第二个等式的证明则使用了在问题 H.11 中为了证明 $q^{1/24}\prod_{k\geqslant 1}(1-q^k) = \sum_{m\in\mathbf{Z}}(-1)^m q^{(6m+1)^2/24}$ 所用的相似的技术, 关键点是它的两端都是权为 1 的模形式 (如果 $q = e^{2i\pi z}$, 第三项则是 $\eta(z)\eta(23z)$, 其中 η 是戴德金 η 函数, 而左边的项则可用雅可比 θ 函数表达).

---

[21] ρ 在 $\mathbf{GL}_2(\mathbf{C})$ 中的像可能会任意大, 因为总可以用一个附属于狄利克雷特征标的线性特征标去对一个表示进行扭变. 相反地, 如果观察 ρ 在 $\mathbf{GL}_2(\mathbf{C})$ 对位似变换的商群 $\mathbf{PGL}_2(\mathbf{C})$ 的像, 这消灭了其自由度, 从而 ρ 的像具有二面体的类型 (一个正多边形的对称群), 同构于 A_4, S_4 或者 A_5. 最难的是 A_5 的情形, 因为这是个单群, 完全不同于那些列出的群, 它们可以由一串交换群逐次解开.

[22] 在附录 C 的图 4 中的 IV 型表示对于 $\mathbf{GL}_2(\mathbf{F}_3)$ 是 2 维的.

[23] 他们是通过证明 J-P. 塞尔 (1984) 的一个更广泛更精细的猜想来得到此结果的, 它作为继朗兰兹和滕内尔的结果之后的课题的所有结果的引导线路, 其中包括了费马大定理的证明.

4.3. 偶表示和 Maass 形式

Maass 形式是比模形式要新近得多的对象, 因为它们仅仅在 1949 年才由 H. Maass 引进.

一个 D 级, 特征标为 χ, 且特征值为 $\lambda \in \mathbf{C}$ 的 Maass 形式 f 是 $\mathscr{H}$(看作 $\mathbf{R}^2$ 上的一个开集) 上的一个 $\mathscr{C}^\infty$ 函数, 并满足以下条件:

(i) 对任意的 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(D)$ 有 $f(\frac{az+b}{cz+d}) = \chi(d)f(z)$.

(ii) $\Delta f = \lambda f$, 其中 $\Delta = -y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})$ 是拉普拉斯算子.

(iii) f 在无限远速降.

一个这样的形式有一个如下类型的傅里叶展开[24]

$$f(z) = \sum_{n \in \mathbf{Z} - \{0\}} a_n(f)\sqrt{y}K_\nu(2\pi|n|y)e^{2i\pi nx},$$

其中 $\frac{1}{4} - \nu^2 = \lambda$ 而 $K_\nu(y) = \frac{1}{2}\int_0^{+\infty} e^{-y(t+t^{-1})/2}t^\nu \frac{dt}{t}$ 是一个贝塞尔函数 (参看习题 IV. 1.9 和问题 H.10), 它的好处之一是当 $\mathrm{Re}(s) > |\mathrm{Re}(\nu)|$ 时满足

$$\int_0^{+\infty} K_\nu(y)y^s \frac{dy}{y} = 2^{s-2}\Gamma(\frac{s+\nu}{2})\Gamma(\frac{s-\nu}{2}).$$

称 f 是偶的即满足 $f(-\bar{z}) = f(z)$, 而奇的即满足 $f(-\bar{z}) = -f(z)$; 对每个 Maass 形式可伴以一个 L 函数, 它的定义公式是 $L(f,s) = \sum_{n=1}^{+\infty} \frac{a_n(f)}{n^s}$, 并有当 f 是偶的时,

$$\int_0^{+\infty} f(iy)y^{s-1/2}\frac{dy}{y} = \pi^{-s}\Gamma(\frac{s+\nu}{2})\Gamma(\frac{s-\nu}{2})L(f,s),$$

而当 f 为奇的时,

$$\int_0^{+\infty} \frac{1}{4i\pi}\frac{\partial f}{\partial x}(iy)y^{s+1/2}\frac{dy}{y} = \pi^{-s}\Gamma(\frac{s+1+\nu}{2})\Gamma(\frac{s+1-\nu}{2})L(f,s).$$

称一个 Maass 形式是本原的是指它的 L 函数具有: [531]

- 一个欧拉因子乘积的展开:

$$L(f,s) = \prod_{p|D} \frac{1}{1 - a_p(f)p^{-s}} \prod_{p\nmid D} \frac{1}{1 - a_p(f)p^{-s} + \chi(p)p^{k-1-2s}},$$

- 一个类型如 $\Lambda(f, k-s) = w\Lambda(f^*, s)$ 的函数方程, 其中 $f^*(z) = \overline{f(-\bar{z})}$, 而 w 是个模为 1 的复数, 又按照 f 偶奇的不同 $c = 0$ 或 1, 最后,

$$\Lambda(f,s) = \pi^{-s}\Gamma(\frac{s+c+\nu}{2})\Gamma(\frac{s+c-\nu}{2})D^{s/2}L(f,s).$$

---

[24] f 所满足的偏微分方程可转换成对于傅里叶系数的二阶微分方程, 这些解中有唯一一个 (差一个常数乘法因子) 不会在无限远激增.

猜想 G.1.6. — 如果 $\rho : \mathscr{G}_{\mathbf{Q}} \to \mathbf{GL}_2(\mathbf{C})$ 是一个偶的不可约表示, 则存在一个特征值为 $\frac{1}{4}$ 的本原 Maass 形式 f, 使得 $L(f,s) = L(\rho,s)$.

这个断言蕴含了对于这样一个表示的阿廷猜想. 鉴于前面提到的朗兰兹和滕内尔的工作, 如果过 ρ 在 $\mathbf{PGL}_2(\mathbf{C})$ 中的像不是 A_5, 那么便可知如何证明它.

5. 类域论

设 F 是个数域[25]. $x \in F$ 被某个首 1 多项式 $P \in \mathbf{Z}[X]$(与 x 相关) 消零的 x 的集合 $\mathcal{O}_F$ 是 F 的一个子环, 称其为整数环. 例如, 如果 $d \in \mathbf{Z}$ 不被任何素数的平方整除, 则 $\mathbf{Q}(\sqrt{d})$ 的整数环是在简介小节中的环 A_D.

这样一个环不一定是主理想的[26], 但是 $\mathcal{O}_F$ 的每个理想 $\mathfrak{n}$ 却可以写成[27] $\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r}$, 其中这些 $\mathfrak{p}_i$ 是不同的素理想[28]. $\mathcal{O}_F$ 的两个理想 $\mathfrak{a}$ 和 $\mathfrak{b}$ 互素 (对任意一个环而言这都意味着 $\mathfrak{a} + \mathfrak{b} = \mathcal{O}_F$) 当且仅当没有 $\mathcal{O}_F$ 中的一个素理想同时出现在 $\mathfrak{a}$ 和 $\mathfrak{b}$ 的素理想分解中.

我们可以将狄利克雷特征标和狄利克雷 L 函数的概念推广到数域上. 如果 $\mathfrak{f}$ 是 $\mathcal{O}_F$ 的一个理想, 以 $I_{\mathfrak{f}}$ 记 $\mathcal{O}_F$ 中与 $\mathfrak{f}$ 互素的理想的集合. 一个 (有限阶的) mod $\mathfrak{f}$ 的赫克特征标 χ 是一个乘性函数 $\chi : I_{\mathfrak{f}} \to \mathbf{C}^*$ 使得, 如果 $\alpha \in \mathcal{O}_F$ 为正[29], 并且 $\alpha - 1 \in \mathfrak{f}$, 则当 $\mathfrak{n}$ 是由 α 生成的主理想时有 $\chi(\mathfrak{n}) = 1$. 与一个 (有限阶) mod $\mathfrak{f}$ 的赫克特征标关联的赫克 L 函数定义为 [532]

$$L(\chi, s) = \sum_{\mathfrak{n} \in I_{\mathfrak{f}}} \frac{\chi(\mathfrak{n})}{N(\mathfrak{n})^s}, \text{ 其中 } N(\mathfrak{n}) = |\mathcal{O}_F/\mathfrak{n}|.$$

由于 χ 是乘性的, 并由于 $\mathfrak{n} \mapsto N(\mathfrak{n})$ 也是乘性的, 那么用对于狄利克雷 L 函数的同一推理便证明了我们有了一个欧拉因子的乘积分解:

$$L(\chi, s) = \prod_{\mathfrak{p} \in \mathscr{P}_F} \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}} = \prod_{p \in \mathscr{P}} \left(\prod_{\mathfrak{p} | (p)} \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}} \right),$$

并由于对几乎所有的 p 有 $\prod_{\mathfrak{p}|(p)} N(\mathfrak{p}) = p^{[F:\mathbf{Q}]}$, 故除了有限个 p 外, 因子 $\prod_{\mathfrak{p}|(p)}(1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s})$ 是对 p^{-s} 的 $[F:\mathbf{Q}]$ 次的多项式.

现将前面所做特别用于把 $\mathcal{O}_F$ 的理想 $\mathfrak{n}$ 带到 1 的平凡特征标. 那么, 与其相伴的赫克 L 函数 $\zeta_F(s) = \sum_{\mathfrak{n}} \frac{1}{N(\mathfrak{n})^s}$ 已为戴德金在很久以前考虑过了; 称它是 F 的戴德金 ζ 函数.

---

[25] 后面的所有陈述都是代数数论的基础性结果, 这绝不意味着它们是容易建立的.

[26] 这与拉梅 (Lamé) 和柯西的希望相反, 他们在 1847 年就费马定理的证明应该属于谁进行的争论直到库默尔提出了一个让每个人都承认的反例才得以停息.

[27] 具有此性质的环是戴德金环.

[28] 如果 I 和 J 是环 A 的两个理想, I 和 J 的乘积 IJ 是 A 的一个理想, 它由所有形如 $ab (a \in I, b \in J)$ 生成. 例如, 如果 I 和 J 是分别由 α 和 β 生成的主理想, 那么 IJ 是由 $\alpha\beta$ 生成的主理想. 另外, 一个理想 $\mathfrak{p}$ 是素的当且仅当 $ab \in \mathfrak{p}$ 蕴含 $a \in \mathfrak{p}$ 或者 $b \in \mathfrak{p}$.

[29] 其意思是, 如果 $\sigma \in \mathscr{G}_{\mathbf{Q}}$ 且 $\sigma(\alpha)$ 为实数, 则有 $\sigma(\alpha) > 0$; 如果 $\sigma(\alpha)$ 不是实数则没有任何条件.

例题 G.1.7. — (i) 如果 $F=\mathbf{Q}$. 我们又回到了黎曼 ζ 函数.

(ii) 如果 $F=\mathbf{Q}[\sqrt{d}]$, 又回到了简介中的函数 ζ_{A_D}.

定理 G.1.8. — (赫克, 1920) *如果 χ 是个本原赫克特征标, 则 $L(\chi,s)$ 具有到整个 $\mathbf{C}$ 的亚纯延拓, 当 χ 是平凡特征标时, 它在除 $s=1$ 上的单极点外全纯.*

这种状况对于任意数域和对于 $\mathbf{Q}$ 是完全一样的. 赫克定理的证明与在习题 VII. 6.6 为证明黎曼 ζ 函数到 $\mathbf{C}$ 的亚纯延拓所利用的思想也是一样的. 然而在 $\mathcal{O}_F$ 中存在单位元则会使得推理更加简洁一些.

类域论的主定理因此可陈述如下.

定理 G.1.9. — *如果 ρ 是 $\mathscr{G}_F$ 的一维表示, 则存在 F 的一个有限阶的赫克特征标 χ, 使得 $L(\mathrm{Ind}_{\mathscr{G}_F}^{\mathscr{G}_{\mathbf{Q}}}\rho,s)=L(\chi,s)$.*

克罗内克–韦伯定理已经是一个深刻的定理了, 然而能给出 $\mathbf{Q}$ 的阿贝尔扩域 (这些是被 $\mathscr{G}_{\mathbf{Q}}$ 的线性特征标的核固定不动的数域) 的对称构造的单位根的存在则会大大减轻证明的难度. 在一般的数域情形, 还不知道是否有这样构造扩域的方法[30], 它 [533] 在很大范围内解释了我们为什么要花那么多时间去证明上面的定理 (设计出它的陈述就已经花了许多时间了). 这个故事是在 1880 年年尾从克罗内克和韦伯开始的, 又由希尔伯特在 1900 年左右继续[31], 而上面的定理则可追溯到 1920 年年尾, 这时 Furtwängler、高木贞治 (Takagi)、阿廷和哈塞做出了实质的贡献[32]. 由于所有这些数学家们和接下来三十多年的数学家们的努力, 我们现在有了一个威力强大的理论, 有了能很好理解的紧凑的陈述, 并且它能很好地充作一个黑匣子. 它成了 M2(数学 2) 的基本课程的常规选项.

G.2. 重返克罗内克–韦伯定理

谢瓦莱 (Chevalley) 想弄明白是否存在从 $\mathbf{Q}$ (分别地, 从 F, 其中 F 为一个数域) 出发直接构造的一个自然的群, 使得它的 1 维表示恰好是它的本原狄利克雷特征标 (分别地, F 的有限阶的赫克特征标). 这导致了去构造下面将要概述的伊代尔 (idèle) 群[33] 、我们将沿历史的反向走一遍 (阿代尔是在阿廷和 Whaples 亲手操作之下诞生的, 比伊代尔晚了 5 年 (它的名字比起 “赋值环” 多了点诗意)), 但最后出现

[30]这是希尔伯特在 1900 年宣布的最后的问题之一 (推广的克罗内克的 “年轻时最亲爱的梦想”), 对此我们依然不知道如何解.

[31]德国学派在这个课题上处在绝对初创的地位, 那个时期的所有文章都是德文的 (其中包括了日本数学家高木贞治).

[32]希尔伯特问题中的三个 (第 9, 11, 12 个) 与这问题有联系.

[33]“idèle” (伊代尔) 这个字来自 “idéal” (包含了此字的全部意思 ······), 20 年后才诞生了 adèle (阿代尔); Roubaud 将阿代尔和伊代尔当作在 “La Belle Hortense”[49] 中的一对孪生姐妹.

[49]“La Belle Hortense” (漂亮的霍顿斯) 是巴黎的一家著名的酒吧书店.

的常常是简单的思想[34]. 阿代尔是在同时考虑 $\mathbf{Q}$ (分别地, 一个数域 F) 的所有完备化时构造出来的, 泰特在他的博士论文 (1950) 中, 按照阿廷指出的方向, 证明了傅里叶分析在阿代尔上是如何自然地证明了狄利克雷 (分别地, 赫克)L 函数的所有那些我们在第 VII 章中遇到的 (分别地, 在 G.1 的 5 小节中提到的) 解析性质.

1. 阿代尔

1.1. 奥斯特洛夫斯基定理

除了记为 $|\ |_\infty$ 的通常范数外, 我们对于每个素数 p 还可以在 $\mathbf{Q}$ 上定义一个 p-adic 范数 $|\ |_p$. 回顾一下: 它的定义按公式是 (参看小词典的 20.4 的第 1 小节) $|\frac{a}{b}|_p = p^{-v_p(a)+v_p(b)}$, 其中 $a, b \in \mathbf{Z} - \{0\}$, 而 $v_p(n)$ 是整除 n 的 p^v 的最大整数 v.

[534] **定理 G.2.1.** — (奥斯特洛夫斯基 (Ostrowski), 1918) $\mathbf{Q}$ 上的一个非平凡范数 $\|\ \|$ 或是等价于通常的 $|\ |_\infty$ 或是等价于对唯一的素数 p 的 p-adic 范数 $|\ |_p$.

证明 先假设存在 $k \in \mathbf{N}$ 使得 $\|k\| > 1$. 由于 $\|1\| = 1$, 三角不等式表明 $\|k\| \leqslant k$, 从而存在 $\alpha \in]0, 1]$ 使得 $\|k\| = k^\alpha$. 设 $m \in \mathbf{N}$. 可将 m 写成以 k 为底的 $m = \sum_{i=0}^n a_i k^i$ 形式, 其中 $a_i \in \{0, 1, \ldots, k-1\}$, 而 $a_n \neq 0$ 表明 $m \geqslant k^n$. 由于 $\|a_i\| \leqslant a_i \leqslant k-1$ 及 $\|k^i\| = \|k\|^i$, 故得到了不等式

$$\|m\| \leqslant (k-1) \sum_{i=1}^{n} k^{i\alpha} = \frac{k-1}{k^\alpha - 1}(k^{(n+1)\alpha} - 1) \leqslant \frac{k^\alpha(k-1)}{k^\alpha - 1} k^{n\alpha} \leqslant C m^\alpha,$$

其中 $C = \frac{k^\alpha(k-1)}{k^\alpha - 1}$ 与 m 无关. 将这个不等式用于 m^n 得到 $\|m\|^n \leqslant C m^{n\alpha}$, 然后取此不等式的 n 次根并取极限得 $\|m\| \leqslant m^\alpha$. 交换 k 和 m 的角色, 推出当 $\|m\| > 1$ 时这个不等式是个等式.

现在, 如果 $m \in \mathbf{N} - \{0\}$, 则存在 $n \in \mathbf{N}$ 使得有 $\|k^n m\| > 1$. 于是有 $\|m\| = \|k^n\|^{-1} \|k^n m\| = k^{-\alpha n}(k^n m)^\alpha = m^\alpha$, 这证明了对于任意的 $m \in \mathbf{N}$ 等式均成立, 然后, 利用范数的乘性和 $\|-1\| = 1$, 于是对任意的 $x \in \mathbf{Q}$ 有 $\|x\| = |x|_\infty^\alpha$. 由此得到, 如果 $k \in \mathbf{N}$ 使得 $\|k\| > 1$, 则 $\|\ \|$ 等价于通常的范数.

在相反的情形我们对所有的素数 ℓ 有 $\|\ell\| \leqslant 1$. 由于假定了 $\|\ \|$ 非平凡, 故至少存在一个素数 p 使得 $\|p\| < 1$. 如果还存在另一个这样的 q, 则对任意的 $n \in \mathbf{N}$, 根据贝祖定理, 可以找到 $u_n, v_n \in \mathbf{Z}$ 使得 $u_n p^n + v_n q^n = 1$, 由此得到

$$1 = \|1\| = \|u_n p^n + v_n q^n\| \leqslant \|u_n\| \cdot \|p\|^n + \|v_n\| \|q\|^n \leqslant \|p\|^n + \|q\|^n.$$

当 n 充分大时这是不可能的. 故存在一个且只有一个素数 p 使得 $\|p\| < 1$, 从而 $\|\ \|$ 等价于 p-adic 范数. 证完. □

下面的结果是整数分解为素数因子乘积的唯一性的直接推论, 但却非常重要; 这表明了利用 $|\ |_p$ 进行正规化的正当性.

[34] 如韦伊所说: "为了跨越所有这些步骤, 好的学生现在只花几天时间而那些在过去要花好几年."

定理 G.2.2. — (乘积公式) 如果 $x \in \mathbf{Q}^*$, 则

$$|x|_\infty \cdot \prod_{p \in \mathscr{P}} |x|_p = 1.$$

1.2. **Q** 的阿代尔环

对于有关 p-adic 数的构造及其初等性质可参看小词典的 20.4 的第 1 节.

设 $\mathscr{V} = \{\infty\} \cup \mathscr{P}$. $\mathscr{V}$ 的元是 $\mathbf{Q}$ 的位 (place). 位 ∞ 是无限远位, 而 $p \in \mathscr{P}$ 则称为有限位. 如果 $v \in \mathscr{V}$, 以 $\mathbf{Q}_v$ 记 $\mathbf{Q}$ 对应的完备化; 因此 $\mathbf{Q}_\infty = \mathbf{R}$.

根据奥斯特洛夫斯基定理, $\mathbf{Q}$ 对于 $v \in \mathscr{V}$ 的完备化就是 $\mathbf{Q}_v$. 我们自然想要考虑所有这些完备化的集合[35]. 可以将 $\mathbf{Q}$ 以对角线的方式嵌入到 $\prod_{v \in \mathscr{V}} \mathbf{Q}_v$ 中, 就是说将 $a \in \mathbf{Q}$ 带到 $(x_v)_{v \in \mathscr{V}}$, 其中对任意的 $v \in \mathscr{V}$ 都有 $x_v = a$. 因此除非 p 整除 a 的分母我们总有 $x_p \in \mathbf{Z}_p$, 这证明了 $\mathbf{Q}$ 的像被包含在 $\prod_{v \in \mathscr{V}} Q_v$ 的一个子环中, 这个子环由 $x = (x_\infty, \dots, x_p, \dots)$ 组成, 其中 $x_p \in \mathbf{Z}_p$ 对几乎所有的 p 成立. 这个环是 $\mathbf{Q}$ 的阿代尔环 $\mathbf{A}$; 这是一个 $\mathbf{Q}_v$ 相对 $\mathbf{Z}_p$ 的, 按 $p \in \mathscr{P}$ 的限制乘积. 我们常常以 $(x_\infty, x^{]\infty[})$ 记 $\mathbf{A}$ 中的元 x, 其中 $x^{]\infty[}$ 是 x 的有限部分 (即在 ∞ 之外). 如果 $v \in \mathscr{V}$, 则可将 $\mathbf{Q}_v$ 等同于 $\mathbf{A}$ 的一个子环, 其元 x 为除了 v 分量外其他分量全为 0. [535]

对 $\mathbf{A}$ 赋予一个限制乘积拓扑, 由取 $\prod_{v \in S} U_v \times \prod_{p \notin S} \mathbf{Z}_p$ 为开集基定义, 其中 S 遍历 $\mathscr{V}$ 的包含 ∞ 的有限子集, 而 $U_v (v \in S)$ 遍历了 $\mathbf{Q}_v$ 的开集. 下面的命题 G.2.3 和 G.2.4 证明了 $\mathbf{Q}$ 在 $\mathbf{A}$ 中离散, 但远非稠密.

命题 G.2.3. — (i) $\mathbf{A}$ 中每个元 x 可以以唯一的方式写成 $x = \alpha + y$ 的形式, 其中 $\alpha \in \mathbf{Q}$, 而 $y \in [0,1[\times \widehat{\mathbf{Z}}$, 其中 $\widehat{\mathbf{Z}} = \prod_{p \in \mathscr{P}} \mathbf{Z}_p$.

(ii) $\mathbf{Q}$ 在 $\mathbf{A}$ 中离散, 而 $\mathbf{A}/\mathbf{Q}$ 为紧的.

证明　我们先证明, 如果这种书写形式存在则唯一. 如果 $\alpha_1 + y_1 = \alpha_2 + y_2$, 其中 $\alpha_1, \alpha_2 \in \mathbf{Q}$, $y_1, y_2 \in [0,1[\times \widehat{\mathbf{Z}}$, 于是特别有 $\alpha_2 - \alpha_1 \in \mathbf{Z}_p$, 其中 $p \in \mathscr{P}$, 因此 $\alpha_2 - \alpha_1 \in \mathbf{Z}$. 但 $\alpha_1 + y_{1,\infty} = \alpha_2 + y_{2,\infty}$ 并由于 $y_{1,\infty}, y_{2,\infty} \in [0,1[$, 故它蕴含了 $\alpha_1 = \alpha_2$, 从而 $y_2 = y_1$. 唯一性得证.

转向存在性的证明. 如果 S 是 $\mathscr{P}$ 的一个有限子集, 使得当 $p \notin S$ 时有 $x_p \in \mathbf{Z}_p$. 又根据小词典的 20.4.3 小节知 $\mathbf{Z}[\frac{1}{p}]$ 在 $\mathbf{Q}_p$ 中稠密, 故对每个 $p \in S$ 存在一个元 $\alpha_p \in \mathbf{Z}[\frac{1}{p}]$, 使得 $x_p - \alpha_p \in \mathbf{Z}_p$. 然而 $x' = x - \sum_{p \in S} \alpha_p \in \mathbf{R} \times \widehat{\mathbf{Z}}$, 从而只需令 $\alpha = [x'_\infty] + \sum_{p \in S} \alpha_p$, $y = x' - [x'_\infty]$(其中 $[x'_\infty]$ 是 x' 在 ∞ 的分量的整数部分) 就能得到 x 的所要形式的分解. (i) 的证明完成.

$\mathbf{Q}$ 的离散性可如此得到: 如果 $x \in \mathbf{A}$, x 的开邻域 $x + (]-\frac{1}{2}, \frac{1}{2}[\times \widehat{\mathbf{Z}})$ 最多包含了 $\mathbf{Q}$ 的一个元, 因为如果有两个这样的元, 它们的差则在 $]-1,1[\times \widehat{\mathbf{Z}}$ 中, 而后者中只有 0 是 $\mathbf{Q}$ 中的元.

[35] 虽说它是自然的, 但在亨泽尔给出 p-adic 数的构造到它的这些后续构造之间竟花了五十多年.

设 $x_1, x_2 \in \mathbf{A}/\mathbf{Q}$ 互不相同, 并设 $\tilde{x}_i = (x_{i,v})(i=1,2)$ 是 x_i 在 $[0,1[\times\widehat{\mathbf{Z}}$ 中的代表形式. 如果 $|x_{1,\infty} - x_{2,\infty}| > 0$, 那么令 $\delta = \min(|x_{1,\infty} - x_{2,\infty}|, 1 - |x_{1,\infty} - x_{2,\infty}|)$, $U_{i,\infty} =]x_{i,\infty} - \frac{1}{3}\delta, x_{i,\infty} + \frac{1}{3}\delta[$ 和 $U_i = U_{i,\infty} \times \widehat{\mathbf{Z}}$, 于是 U_i 是 $\mathbf{A}$ 中包含了 $\tilde{x}_i$ 的开集. 设 $V = \{a - b, a \in U_1, b \in U_2\}$. 由它的构造知 V 包含在 $]\frac{1}{3}\delta, 1 - \frac{1}{3}\delta[\times\widehat{\mathbf{Z}}$ 中; 而它与 $\mathbf{Q}$ 的交因此包含在 $]\frac{1}{3}\delta, 1 - \frac{1}{3}\delta[\cap\mathbf{Z} = \emptyset$ 中, 于是 V 不包含 $\mathbf{Q}$ 中的任何元. 由此推出 $\{a + q_1, a \in U_1\}$ 和 $\{b + q_2, b \in U_2\}$ 对于任意 $q_1, q_2 \in \mathbf{Q}$ 不相交, 从而 U_1 和 U_2 在 $\mathbf{A}/\mathbf{Q}$ 中的像是分别包含 x_1, x_2 的不相交的开集.

如果 $x_{1,\infty} = x_{2,\infty} = c$, 则存在素数 p 和 $n \in \mathbf{N}$ 使得 $x_{1,p}$ 和 $x_{2,p}$ 的 mod p^n 约化互不相同. 以 U_i 记开集 $]c - \frac{1}{2}, c + \frac{1}{2}[\times(x_{i,p} + p^n\mathbf{Z}_p) \times \prod_{\ell\in\mathscr{P}-\{p\}}\mathbf{Z}_\ell$. 因此 V 包含在 $]-1,1[\times((x_{1,p} - x_{2,p}) + p^n\mathbf{Z}_p) \times \prod_{\ell\in\mathscr{P}-\{p\}}\mathbf{Z}_\ell$ 中, 于是不包含 $\mathbf{Q}$ 中的任何元 ($V \cap \mathbf{Q}$ 中的一个元 q 属于 $(\mathbf{R}\times\widehat{\mathbf{Z}}) \cap \mathbf{Q} = \mathbf{Z}$, 满足 $|q| < 1$, 从而 $q = 0$, 这与它属于 $(x_{1,p} - x_{2,p}) + p^n\mathbf{Z}_p$ 不合). 由于以上原因, 这给我们提供了 $\mathbf{A}/\mathbf{Q}$ 的分别包含了 x_1 和 x_2 的不相交的开集.

由此也得到 $\mathbf{A}/\mathbf{Q}$ 是分离的. 最后, 从 $\mathbf{A}$ 到 $\mathbf{A}/\mathbf{Q}$ 的投射在 $[0,1]\times\widehat{\mathbf{Z}}$ 上的限制是满的. [536] 由于 $[0,1]\times\widehat{\mathbf{Z}}$ 作为紧集的乘积为紧的 (甚至可作为度量紧集的可数乘积) 以及 $\mathbf{A}/\mathbf{Q}$ 为分离的, 这便证明了 $\mathbf{A}/\mathbf{Q}$ 作为紧集的连续函数的像为紧的. □

如果 $S = \{p_1, \ldots, p_s\}$ 是 $\mathscr{P}$ 的一个有限子集, 记 $\mathbf{Z}[S^{-1}]$ 为 $\mathbf{Q}$ 的子环 $\mathbf{Z}[\frac{1}{p_1}, \ldots, \frac{1}{p_s}]$, 这是令 $p_1, \ldots, p_s$ 可逆得到的.

命题 G.2.4. — *如果 $S \subset \mathscr{P}$ 为有限集, 则 $\mathbf{Z}[S^{-1}]$ 在 $\prod_{p\in S}\mathbf{Q}_p$ 中稠密.*

证明 由于 p_i^n 之间两两互素, 根据中国剩余定理故存在 mod p_i^n 同余于 1, 而 mod $p_j^n (j \in S - \{i\})$ 同余于 0 的 $a_{i,n} \in \mathbf{Z}$. 如果现在 $y_i \in \mathbf{Q}_{p_i}$, 根据小词典的 20.4.3 节, 由于 $\mathbf{Z}[\frac{1}{p_i}]$ 在 $\mathbf{Q}_{p_i}$ 中稠密, 故可以找到 $x_{i,n} \in \mathbf{Z}[\frac{1}{p_i}]$ 使得 $|x_{i,n} - y_i| \leqslant p_i^{-n}$. 令 $x_n = \sum_{j=1}^s a_{j,n}x_{j,n}$, 给出了 $\mathbf{Z}[S^{-1}]$ 中的一个序列, 其满足

$$\begin{aligned}
|x_n - y_i|_{p_i} &= |a_{i,n}x_{i,n} - y_i + \sum_{j\neq i} a_{j,n}x_{j,n}|_{p_i} \\
&= |a_{i,n}(x_{i,n} - y_i) + (a_{i,n} - 1)y_i + \sum_{j\neq i} a_{j,n}x_{j,n}|_{p_i} \\
&\leqslant \sup(|a_{i,n}|_{p_i}|(x_{i,n} - y_i)|_{p_i}, |(a_{i,n} - 1)|_{p_i}|y_i|_{p_i}, \sup_{j\neq i}|a_{j,n}|_{p_i}|x_{j,n}|_{p_i}).
\end{aligned}$$

现在, 当 $j \neq i$ 时我们有 $|x_{j,n}|_{p_i} \leqslant 1$, 并且因为 $|(x_{i,n} - y_i)|_{p_i}, |(a_{i,n} - 1)|_{p_i}, |a_{j,n}|_{p_i}$ 当 $j \neq i$ 时均 $\leqslant p_i^{-n}$, 可看出 x_n 在 $\prod_{p\in S}\mathbf{Q}_p$ 中趋向 $(y_1, \ldots, y_s)$. 得到结论. □

1.3. Q 的伊代尔群

$\mathbf{Q}$ 的伊代尔群 $\mathbf{A}^*$ 是环 $\mathbf{A}$ 中的可逆元的群; 因此它是 $(x_v)_{v\in\mathscr{V}}$ 的集合, 其中 $x_v \in \mathbf{Q}_v^*$, 且对几乎所有的 $p \in \mathscr{P}$ 有 $x_p \in \mathbf{Z}_p^*$; 换言之, $\mathbf{A}^*$ 是相对于 $\mathbf{Z}_p^*(p \in \mathscr{P})$ 而言的 $\mathbf{Q}_v^*$ 的限制乘积; 我们赋予限制乘积的拓扑, 其开集基由 $\prod_{v\in S}U_v \times \prod_{p\notin S}\mathbf{Z}_p^*$ 构成,

其中 S 遍历 $\mathscr{V}$ 的包含了 ∞ 的有限子集, 而 $U_v(v \in S)$ 为 $\mathbf{Q}_v^*$ 的开集.

如果 $\beta \in \mathbf{Q}^*$, 则除了 p 整除 β 的分母或分子外都有 $\beta \in \mathbf{Z}_p^*$, 这证明了 $\prod_{v \in \mathscr{V}} \mathbf{Q}_v$ 的元 $(\beta, \beta, \ldots)$ 属于 $\mathbf{A}^*$. 从而可以将 $\mathbf{Q}^*$ 等同于 $\mathbf{A}^*$ 的一个子群. 如果 $v \in \mathscr{V}$, 则可将 $\mathbf{Q}_v^*$ 等同于 $\mathbf{A}$ 中那些除了在 v 的分量外其余分量全为 1 的 x 组成的子群.

如果 $x = (x_v)_{v \in \mathscr{V}} \in \mathbf{A}^*$, 则对于几乎所有的 p 有 $|x_p|_p = 1$, 这让我们可以定义 $|x|_{\mathbf{A}}$ 为 $|x|_{\mathbf{A}} = \prod_{v \in \mathscr{V}} |x_v|_v$. 对于任意的 $\beta \in \mathbf{Q}^*$, 由乘积公式 (定理 G.2.2) 得到 $|\beta|_{\mathbf{A}} = 1$.

引理 G.2.5. — (i) $\mathbf{A}^*$ 中所有的元 x 可以以唯一的方式写为 $x = \beta b_\infty b^{]\infty[}$ 的形式, 其中 $\beta \in \mathbf{Q}^*$, $b_\infty \in \mathbf{R}_+^*$, 而 $b^{]\infty[} \in \widehat{\mathbf{Z}^*}$, 其中 $\widehat{\mathbf{Z}^*} = \prod_{p \in \mathscr{P}} \mathbf{Z}_p^*$.

(ii) $\mathbf{A}^*/\mathbf{Q}^* \cong \mathbf{R}_+^* \times \widehat{\mathbf{Z}^*}$.

证明 我们可以令 $\beta = \operatorname{sign}(x_\infty) \prod_{p \in \mathscr{P}} p^{v_p(x_p)}$, 于是 $b = \beta^{-1} x$ 满足条件 $b_\infty \in \mathbf{R}_+$ 和 $b^{]\infty[} \in \prod_{p \in \mathscr{P}} \mathbf{Z}_p^*$. 由此得到了 (i), 而 (ii) 是个直接推论. □

2. 阿代尔上的泊松公式

[537]

2.1. $\mathbf{Q}_p$ 上的傅里叶变换

如果 $p \in \mathscr{P}$, 记 $\mathscr{S}(\mathbf{Q}_p)$ 是取值在 $\mathbf{C}$ 中的那样的函数的空间 (施瓦兹 (Schwartz) 空间), 它们是局部常值的且具有在 $\mathbf{Q}_p$ 中的紧支集. 设 $\phi \in \mathscr{S}(\mathbf{Q}_p)$. 由于 ϕ 具有紧支集 (从而有界), 故存在 $m \in \mathbf{Z}$ 使得当 $|x|_p > p^{-m}$ 时有 $\phi(x) = 0$; 换句话说, 存在 $m \in \mathbf{Z}$ 使得当 $x \notin p^m \mathbf{Z}_p$ 时 $\phi(x) = 0$. 另外, 由于 ϕ 为局部常值, 故对每个 $x \in p^m \mathbf{Z}_p$ 存在整数 $n_x \in \mathbf{N}$, 使得 ϕ 在 $B(x, p^{-n_x}) = x + p^{n_x} \mathbf{Z}_p$ 为常值. 因为 $p^m \mathbf{Z}_p$ 为紧集, 故可从这些 $x + p^{n_x} \mathbf{Z}_p$ 中挑出 $p^m \mathbf{Z}_p$ 的一个有限覆盖. 以 n 记这个有限覆盖所涉及的 n_x 中的最小者, 于是可以说, 存在 $n \in \mathbf{N}$ 使得对任意的 $x \in p^m \mathbf{Z}_p$, ϕ 在 $x + p^n \mathbf{Z}_p$ 上为常值. 以 $\mathbf{1}_{a + p^n \mathbf{Z}_p}$ 记 $a + p^n \mathbf{Z}_p$ 的特征函数并利用 $\mathbf{Z}[\frac{1}{p}]$ 在 $\mathbf{Q}_p$ 中的稠密性, 由此便得到下面的结果.

命题 G.2.6. — $\mathscr{S}(\mathbf{Q}_p)$ 是由这些 $\mathbf{1}_{a + p^n \mathbf{Z}_p}$ 生成的向量空间, 其中 $a \in \mathbf{Z}[\frac{1}{p}]$ 而 $n \in \mathbf{N}$. 另外, 这些 $\mathbf{1}_{a + p^n \mathbf{Z}_p}$ 之间的关系由以下的这些关系生成:

- 如果 $b \in a + p^n \mathbf{Z}$, 则 $\mathbf{1}_{a + p^n \mathbf{Z}_p} = \mathbf{1}_{b + p^n \mathbf{Z}_p}$,
- $\mathbf{1}_{a + p^n \mathbf{Z}_p} = \sum_{i=0}^{p-1} \mathbf{1}_{a + i p^n + p^{n+1} \mathbf{Z}_p}$,

其中的第二个翻译过来是说, 如果我们知道了除以 p^n 的余数, 那么除以 p^{n+1} 的余数有 p 种可能性.

如果 $\phi \in \mathscr{S}(\mathbf{Q}_p)$, 我们令 $\int_{\mathbf{Q}_p} \mathbf{1}_{a + p^n \mathbf{Z}_p}(x) dx = p^{-n}$, 其中 $a \in \mathbf{Z}[\frac{1}{p}], n \in \mathbf{N}$, 然后按线性性定义 $\int_{\mathbf{Q}_p} \phi(x) dx$, 这等于要求 $\mathbf{Z}_p$ 的测度为 1 以及积分在平移下的不变性 (即是一个哈尔测度). 由于这些 $\mathbf{1}_{a + p^n \mathbf{Z}_p}$ 之间仅有的关系就是上面那些, 故这个定义是可能的.

如果 $x \in \mathbf{Q}_p$, 则存在 $\xi \in \mathbf{Z}[\frac{1}{p}]$ 使得 $x-\xi \in \mathbf{Z}_p$(这是 $\mathbf{Z}[\frac{1}{p}]$ 在 $\mathbf{Q}_p$ 中的稠密性的推论), 而且 ξ 被确定到一个 $\mathbf{Z}[\frac{1}{p}] \cap \mathbf{Z}_p = \mathbf{Z}$ 的加法项. 由此知道 $e^{2i\pi\xi}$ 只依赖 x 而不依赖 ξ 的选取, 这让我们可以将它记为 $e^{2i\pi x}$. 于是立即可知, $x \mapsto e^{2ix\pi}$ 是 $\mathbf{Q}_p$ 的一个线性特征标 ($e^{2i\pi(x+y)} = e^{2i\pi x}e^{2i\pi y}$), 它是局部常值的 (对于所有 $a \in \mathbf{Q}_p$, 在 $a+\mathbf{Z}_p$ 上为常值).

那么, 我们以下面的公式定义 $\phi \in \mathscr{S}(\mathbf{Q}_p)$ 的傅里叶变换 $\hat{\phi} = \mathscr{F}_p\phi$:

$$\hat{\phi}(y) = \int_{\mathbf{Q}_p} \phi(x)e^{2i\pi xy}dx.$$

由于 $x \mapsto \phi(x)e^{2i\pi xy}$ 与 ϕ 的支集相同, 并且作为两个局部常值函数的乘积仍为常值, 故上面的定义是有意义的.

例题 G.2.7. — (i) $\mathbf{1}_{\mathbf{Z}_p}$ 的傅里叶变换是 $\mathbf{1}_{\mathbf{Z}_p}$. 事实上, 如果 $y \in \mathbf{Z}_p$, 则对于任意的 $x \in \mathbf{Z}_p$ 有 $e^{2i\pi xy} = 1$, 从而 $\int_{\mathbf{Q}_p} \mathbf{1}_{\mathbf{Z}_p}(x)e^{2i\pi xy}dx = \int_{\mathbf{Q}_p} \mathbf{1}_{\mathbf{Z}_p}(x)dx = 1$. 相反地, 如果 [538] $v_p(y) = -n < 0$, 那么 $\mathbf{Z}_p$ 的线性特征标 $x \mapsto e^{2i\pi xy}$ 非平凡并且 mod $p^n\mathbf{Z}_p$ 为常值; 因此从有限群的线性特征标的正交性以及 $a \mapsto e^{2i\pi ya}$ 是 $\mathbf{Z}_p/p^n\mathbf{Z}_p \cong \mathbf{Z}/p^n\mathbf{Z}$ 的非平凡线性特征标得到

$$\int_{\mathbf{Q}_p} \mathbf{1}_{\mathbf{Z}_p}(x)e^{2i\pi xy}dx = \int_{\mathbf{Q}_p} \sum_{a \in \mathbf{Z}_p/p^n\mathbf{Z}_p} e^{2i\pi ya}\mathbf{1}_{a+p^n\mathbf{Z}_p}(x)dx = p^{-n} \sum_{a \in \mathbf{Z}_p/p^n\mathbf{Z}_p} e^{2i\pi ya} = 0.$$

(ii) 同样的计算证明, 如果 ϕ 是 mod $p^n\mathbf{Z}_p$ 常值并其支集在 $p^{-m}\mathbf{Z}_p$ 中, 那么 $\hat{\phi}$ 为 mod $p^m\mathbf{Z}_p$ 常值, 并且其支集在 $p^{-n}\mathbf{Z}_p$ 中.

(iii) 设 $\chi : (\mathbf{Z}/p^n\mathbf{Z})^* \to \mathbf{C}^*$ 是导子 p^n 的狄利克雷特征标, 其中 $n \geqslant 1$. 利用同构 $\mathbf{Z}_p/p^n\mathbf{Z}_p \cong \mathbf{Z}/p^n\mathbf{Z}$ 可以伴以 χ 一个函数 ϕ_χ, 使其支集在 $\mathbf{Z}_p$ 中 (甚至在 $\mathbf{Z}_p^*$ 中), 且为 mod $p^n\mathbf{Z}_p$ 常值: 而当 $x \in p\mathbf{Z}_p$ 时令 $\phi_\chi(x) = 0$, 而当 $x \in \mathbf{Z}_p^*$ 时令 $\phi_\chi(x) = \chi(\bar{x})$, 其中 $\bar{x}$ 是 x 的 mod $p^n\mathbf{Z}_p$ 的像. 于是 ϕ_χ 的傅里叶变换由公式

$$\hat{\phi}_\chi(y) = \frac{G(\chi)}{p^n}\phi_{\bar{\chi}}(p^n y)$$

定义, 其中

$$G(\chi) = \sum_{a \in (\mathbf{Z}/p^n\mathbf{Z})^*} \chi(a)e^{2i\pi \frac{a}{p^n}}$$

是在 VII.4 的 2 小节中引进的高斯和. 实际上, ϕ_χ 作为 mod $p^n\mathbf{Z}_p$ 常值的特征标, 则 $\hat{\phi}_\chi$ 在 $p^{-n}\mathbf{Z}_p$ 之外为 0, 并且当 $v_p(y) \geqslant -n$ 时, 此公式等价于引理 VII.4.3 中的公式.

$\mathbf{Q}_p$ 上的傅里叶变换满足与在 $\mathbf{R}$ 上关于伸缩、平移 …… 有同样的性质. 准确地说, 有以下结果.

命题 G.2.8. — (i) 如果 $a \in \mathbf{Q}_p^*$ 而 $b, c \in \mathbf{Q}_p$, 则

$$\mathscr{F}_p(\phi(ax))(y) = |a|_p^{-1}\hat{\phi}(a^{-1}y),$$

$$\mathscr{F}_p(\phi(x+b))(y) = e^{-2i\pi by}\hat{\phi}(y) \quad 和 \quad \mathscr{F}_p(e^{2i\pi cx}\phi(x))(y) = \hat{\phi}(y+c).$$

(ii) $(\mathscr{F}_p \circ \mathscr{F}_p\phi)(x) = \phi(-x)$ (傅里叶反演公式).

证明　如果 $a \in \mathbf{Q}_p^*$ 而 $b, c \in \mathbf{Q}_p$, 令 $u_{a,b,c} : \mathscr{S}(\mathbf{Q}_p) \to \mathscr{S}(\mathbf{Q}_p)$ 为 $(u_{a,b,c}\phi)(x) = e^{2i\pi cx}\phi(ax+b)$. 在定义 $\mathscr{F}_p \circ u_{a,b,c}$ 的积分中的变量变换立即证明

$$\mathscr{F}_p \circ u_{a,b,c} = |a|_p^{-1} e^{-2i\pi\frac{bc}{a}} u_{a^{-1},a^{-1}c,-a^{-1}b} \circ \mathscr{F}_p.$$

于是得到了 (i). 将 (i) 用两次则证明了 $\mathscr{F}_p \circ \mathscr{F}_p \circ u_{a,b,c} = u_{a,-b,-c} \circ \mathscr{F}_p \circ \mathscr{F}_p$. 设 Y 是 $\mathscr{S}(\mathbf{Q}_p)$ 中那些函数 ϕ 组成的子空间, 它们满足 $\mathscr{F}_p \circ \mathscr{F}_p\phi = u_{-1,0,0}\phi$. 由于 $u_{a,-b,-c} \circ u_{-1,0,0} = u_{-1,0,0} \circ u_{a,b,c}$, 由此看出 Y 在 $u_{a,b,c}$ 下稳定. 另外, Y 包含了 $\mathbf{1}_{\mathbf{Z}_p}$, 同时 $u_{p^{-n},-p^n a,0}\mathbf{1}_{\mathbf{Z}_p} = \mathbf{1}_{a+p^n\mathbf{Z}_p}$, 因此 Y 包含了 $\mathbf{1}_{a+p^n\mathbf{Z}_p}$, 其中 $a \in \mathbf{Q}_p, n \in \mathbf{Z}$, 从而 $Y = \mathscr{S}(\mathbf{Q}_p)$. 得到结论. □

2.2. 阿代尔上的傅里叶变换

设 $\mathscr{S}(\mathbf{A})$ 是 $\mathbf{A}$ 的施瓦兹空间. 它是形如 $\phi(x) = \prod_{v\in S}\phi_v(x_v)\prod_{p\notin S}\mathbf{1}_{\mathbf{Z}_p}(x_p)$ 的函数 ϕ 的线性组合的集合, 其中 S 遍历 $\mathscr{V}$ 的包含 ∞ 的有限子集, 而当 $v \in S$ 时 $\phi_v \in \mathscr{S}(\mathbf{Q}_v)$. 这样的一个函数也被记为 $\otimes_{v\in\mathscr{V}}\phi_v$, 其中暗含着对几乎所有的 $p \in \mathscr{P}$ 有 $\phi_p = \mathbf{1}_{\mathbf{Z}_p}$ 的意思. [539]

由于这些 $\mathbf{1}_{a+p^n\mathbf{Z}_p}$ 生成了 $\mathscr{S}(\mathbf{Q}_p)$, 那么可看出 $\mathscr{S}(\mathbf{A})$ 也就由如下函数生成:

$$\phi_\infty(x_\infty)\prod_{p\in S}\mathbf{1}_{a_p+p^{n_p}\mathbf{Z}_p}(x_p)\prod_{p\notin S}\mathbf{1}_{\mathbf{Z}_p}(x_p) = \phi_\infty(x_\infty)\mathbf{1}_{a+N\widehat{\mathbf{Z}}}(x^{]\infty[}),$$

其中 $N = \prod_{p\in S}p^{n_p}$, 而 a 是 $\mathbf{Z}[S^{-1}]$ 中使得对任意的 $p \in S$ 有 $a - a_p \in \mathbf{Z}_p$ 的元 (这样一个 a 的存在性由引理 G.2.4 保证). 另外, 这些生成元之间的关系也由下面这些关系生成 (更简单地, 以 $\phi_\infty \otimes \mathbf{1}_{a+N\widehat{\mathbf{Z}}}$ 记出现在上面右端中的 $\mathscr{S}(\mathbf{A})$ 中的元):

- 如果 $a - b \in N\mathbf{Z}$, 则 $\phi_\infty \otimes \mathbf{1}_{a+N\widehat{\mathbf{Z}}} = \phi_\infty \otimes \mathbf{1}_{b+N\widehat{\mathbf{Z}}}$,
- 如果 $a \in \mathbf{Q}, M, N \in \mathbf{N} - \{0\}$, 则 $\phi_\infty \otimes \mathbf{1}_{a+N\widehat{\mathbf{Z}}} = \sum_{i=0}^{M-1}\phi_\infty \otimes \mathbf{1}_{a+iN+NM\widehat{\mathbf{Z}}}$.

如果 $\phi \in \mathscr{S}(\mathbf{A})$, 令 $\int_{\mathbf{A}}\phi_\infty \otimes \mathbf{1}_{a+N\widehat{\mathbf{Z}}}dx = \frac{1}{N}\int_{\mathbf{R}}\phi_\infty(x_\infty)dx_\infty$, 然后由线性性定义积分 $\int_{\mathbf{A}}\phi dx$, 这意味要求 $[0,1[\times\widehat{\mathbf{Z}}$ 的测度为 1, 且在 $\mathbf{A}$ 上的积分在平移下不变. 我们将注意到, 如果 $\phi = \otimes_{v\in\mathscr{V}}\phi_v$, 则 $\int_{\mathbf{A}}\phi dx = \prod_{v\in\mathscr{V}}\int_{\mathbf{Q}_v}\phi_v(x_v)dx_v$, 其中几乎所有的乘积因子都取 1.

如果 $x = (x_v)_{v\in\mathscr{V}} \in \mathbf{A}$, 我们定义 $e^{2i\pi x}$ 为 $e^{2i\pi x} = e^{-2i\pi x_\infty}\prod_{p\in\mathscr{P}}e^{2i\pi x_p}$, 其中乘积的几乎所有的项等于 1. 直接由定义知, 当 $x, y \in \mathbf{A}$ 时有 $e^{2i\pi(x+y)} = e^{2i\pi x}e^{2i\pi y}$. 另外, 不难验证 $e^{2i\pi(x+\nu)} = e^{2i\pi x}$, 其中 $\nu \in \mathbf{Z}$ 或者 ν 具有 $\frac{1}{p^n}(p \in \mathscr{P}, n \in \mathbf{N})$ 的形式. 由于 $\mathbf{Q}$ 中所有的元都可以写成这种类型的元的和 (分解为简单元), 由此得到 $x \mapsto e^{2i\pi x}$ 是以 $\mathbf{Q}$ 为周期的周期函数.

我们定义 $\phi \in \mathscr{S}(\mathbf{A})$ 的阿代尔傅里叶变换 $\hat{\phi} = \mathscr{F}_{\mathbf{A}}\phi$ 为 $\hat{\phi}(y) = \int_{\mathbf{A}}\phi(x)e^{2i\pi xy}dx$. 如果 $\phi = \otimes_{v\in\mathscr{V}}\phi_v$, 则显然有 $\mathscr{F}_{\mathbf{A}}\phi = \otimes_{v\in\mathscr{V}}\mathscr{F}_v\phi_v$ (因为对几乎所有的 p 有 $\phi_p = \mathbf{1}_{\mathbf{Z}_p}$, 而 $\mathscr{F}_p\phi_p = \mathbf{1}_{\mathbf{Z}_p}$, 故这个表达式是有意义的).

由此得到局部的傅里叶反演公式 (即在 $\mathbf{R}$ 和在 $\mathbf{Q}_p$ 上的意思) 和局部的伸缩公式:

$(\mathscr{F}_{\mathbf{A}} \circ \mathscr{F}_{\mathbf{A}}\phi)(y) = \phi(-y)$ 以及当 $b \in \mathbf{A}^*$ 时有 $\mathscr{F}_{\mathbf{A}}(\phi(bx))(y) = |b|_{\mathbf{A}}^{-1}\hat{\phi}(b^{-1}y)$.

定理 G.2.9. — (泊松公式) 设 $\phi \in \mathscr{S}(\mathbf{A})$, 则

(i) $\sum_{\alpha\in\mathbf{Q}} \phi(\alpha) = \sum_{\alpha\in\mathbf{Q}} \hat{\phi}(\alpha)$.

(ii) 更一般地, 如果 $b \in \mathbf{A}^*$, 则 $\sum_{\alpha\in\mathbf{Q}} \phi(\alpha b) = |b|_{\mathbf{A}}^{-1} \sum_{\alpha\in\mathbf{Q}} \hat{\phi}(\alpha b^{-1})$.

证明　由线性性, 可假设 $\phi = \phi_\infty \otimes \mathbf{1}_{a+N\hat{\mathbf{Z}}}$, 其中 $a \in \mathbf{Q}, N \in \mathbf{N}$. 在这种情形下, $\hat{\phi}(y) = N^{-1}\phi(y_\infty)e^{2i\pi \alpha y^{]\infty[}}\mathbf{1}_{N^{-1}\hat{\mathbf{Z}}}$, 从而化成证明恒等式

$$\sum_{\alpha\in a+N\mathbf{Z}} \phi_\infty(\alpha) = \frac{1}{N} \sum_{\alpha\in N^{-1}\mathbf{Z}} e^{2i\pi a\alpha}\hat{\phi}_\infty(\alpha),$$

将经典的泊松公式 (定理 IV.3.18) 用于函数 $f: \mathbf{R} \to \mathbf{C}(f(x) = \phi_\infty(Nx+a))$, 其傅里叶变换为 $\hat{f}(y) = \frac{1}{N}e^{2i\pi\frac{ay}{N}}\hat{\phi}_\infty(\frac{y}{N})$, 便得到上面的恒等式.

(ii) 由 $x \mapsto \phi_b(x) = \phi(bx)$ 的傅里叶变换 $\hat{\phi}_b(y) = |b|_{\mathbf{A}}^{-1}\hat{\phi}(b^{-1}y)$ 得到. □

[540] 3. 阿代尔上的梅林变换和 L 函数

3.1. 在 $\mathbf{Q}_p^*$ 上的积分

设 $\mathscr{L}_0(\mathbf{Q}_p^*)$ 为那些在 $\mathbf{Q}_p^*$ 中具有紧支集的局部常值函数 ϕ 的集合 (换句话说是 $\mathscr{S}(\mathbf{Q}_p)$ 的一个满足 $\phi(0) = 0$ 的子空间). 如果 $\phi \in \mathscr{L}_0(\mathbf{Q}_p^*)$, 定义 $\int_{\mathbf{Q}_p^*}$ 为

$$\int_{\mathbf{Q}_p^*} \phi(x)d^*x = \frac{p}{p-1}\int_{\mathbf{Q}_p} \phi(x)|x|_p^{-1}dx,$$

这等于说要求了 $\mathbf{Z}_p^*$ 的测度为 1 以及在 $\mathbf{Q}_p^*$ 上的积分在 $x \mapsto bx (b \in \mathbf{Q}_p^*)$ 下不变.

设 $\mathscr{L}(\mathbf{Q}_p^*)$ 是那些函数 $\phi: \mathbf{Q}_p^* \to \mathbf{C}$ 的集合, 它们具有在 $\mathbf{Q}_p$ 中的紧支集, 而对任意的 $n \in \mathbf{Z}$, 它在 $p^n\mathbf{Z}_p^* = \{x, |x|_p = p^{-n}\}$ 上的限制属于 $\mathscr{L}_0(\mathbf{Q}_p^*)$, 并且还是可和的, 意思是说 $\sum_{n\in\mathbf{Z}}\int_{p^n\mathbf{Z}_p^*} |\phi(x)|d^*x < +\infty$. 如果 $\phi \in \mathscr{L}(\mathbf{Q}_p^*)$, 定义 $\int_{\mathbf{Q}_p^*}\phi(x)d^*x$ 为

$$\int_{\mathbf{Q}_p^*} \phi(x)d^*x = \sum_{n\in\mathbf{Z}}\int_{p^n\mathbf{Z}_p^*} \phi(x)d^*x.$$

3.2. 在伊代尔群上的积分

设 $\mathscr{L}(\mathbf{R}^*)$ 是函数 $\phi: \mathbf{R}^* \to \mathbf{C}^*$ 的集合: 它们在无限远是速降的并使得 $\int_{\mathbf{R}^*}|\phi(t)|d^*t < +\infty$, 其中我们令 $d^*t = \frac{dt}{|t|}$. 测度 d^*t 在变量变换 $t \mapsto bt$ $(b \in \mathbf{R}^*)$ 下不变.

设 $\mathscr{L}_0(\mathbf{A}^*)$ 是形如 $\phi(x) = \prod_{v\in\mathscr{V}}\phi_v(x_v)$ 的函数的空间, 其中 $\phi_\infty \in \mathscr{L}(\mathbf{R}^*), \phi_p \in \mathscr{L}_0(\mathbf{Q}_p^*)$, 并且对几乎所有的 p 有 $\phi_p = \mathbf{1}_{\mathbf{Z}_p^*}$. 我们将这个类型的函数记为 $\otimes_{v\in\mathscr{V}}\phi_v$ 的

形式, 并暗含了对几乎所有的 p 有 $\phi_p = \mathbf{1}_{\mathbf{Z}_p^*}$. 如果 $\phi \in \mathscr{L}_0(\mathbf{A}^*)$, 令

$$\int_{\mathbf{A}^*} \otimes_{v\in\mathscr{V}} \phi_v d^*x = \prod_{v\in\mathscr{V}} (\int_{\mathbf{Q}_v^*} \phi_v(x_v) d^*x_v),$$

其中乘积中几乎所有的项都等于 1; 然后利用线性性定义 $\int_{\mathbf{A}^*} \phi(x) d^*x$. 这等于要求了 $[1, a[\times \widehat{\mathbf{Z}}^*$ 的测度是 $\log a$, 而 d^*x 在 $x \mapsto bx$ $(b \in \mathbf{A}^*)$ 下不变.

以 $\mathscr{L}(\mathbf{A}^*)$ 记函数 ϕ 的空间: 它们在 $\beta \mathbf{R}_+^* \widehat{\mathbf{Z}}^*$ 上的限制属于 $\mathscr{L}_0(\mathbf{A}^*)$, 其中 $\beta \in \mathbf{Q}^*$, 另外, 它们是可和的, 即 $\sum_{\beta\in\mathbf{Q}^*} \int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*} |\phi(x)| d^*x < +\infty$. 如果 $\phi \in \mathscr{L}(\mathbf{A}^*)$, 定义

$$\int_{\mathbf{A}^*} \phi(x) d^*x = \sum_{\beta\in\mathbf{Q}^*} \int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*} \phi(x) d^*x.$$

命题 G.2.10. — 设 $\phi_v \in \mathscr{L}(\mathbf{Q}_v^*), v \in \mathscr{V}$, 满足:

- 对几乎所有的 p, 在 $\mathbf{Z}_p^*$ 上有 $\phi_p = 1$,
- $\prod_{v\in\mathscr{V}} (\int_{\mathbf{Q}_v^*} |\phi_v(x_v)| d^*x_v) < +\infty$.

则定义 $\phi : \mathbf{A}^* \to \mathbf{C}$ 为 $\phi(x) = \prod_{v\in\mathscr{V}} \phi_v(x_v)$, 函数 ϕ 是 $\mathscr{L}(\mathbf{A}^*)$ 中的元, 并且 [541] $\int_{\mathbf{A}^*} \phi(x) d^*x = \prod_{v\in\mathscr{V}} (\int_{\mathbf{Q}_v^*} \phi_v(x_v) d^*x_v)$.

证明　如果 $\beta \in \mathbf{Q}^*$, ϕ 在 $\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*$ 上的限制是 $\mathbf{1}_{\mathbf{R}^*_{\mathrm{sign}\beta}} \phi_\infty$ 和那些 $\mathbf{1}_{p^{v_p(\beta)}\mathbf{Z}_p^*} \phi_p$, 并且由于对几乎所有的 p 有 $v_p(\beta) = 0$, 而在 $\mathbf{Z}_p^*$ 上对几乎所有的 p 有 $\phi_p = 1$, 故这个限制明显地是 $\mathscr{L}_0(\mathbf{A}^*)$ 中的元.

剩下的可像命题 VII.3.1 那样证明. 设 $\mathscr{P}(X)$ 是 $\leqslant X$ 的素数的集合, $I(X)$ 为那些 $\beta \in \mathbf{Q}^*$ 的集合, 它们可正可负, 其素因子分解只涉及 $\mathscr{P}(X)$ 中的元, 又令 $I(X, k)$ 为 $\beta \in I(X)$ 并使得 $-k \leqslant v_p(\beta) \leqslant k$ $(p \in \mathscr{P}(X))$ 的集合. 以 $C_p(-k, k)$ 代表环形 $\{x \in \mathbf{Q}_p, p^{-k} \leqslant |x_p| \leqslant p^k\}$, 于是得到

$$\sum_{\beta\in I(X,k)} \int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*} |\phi(x)| d^*x = \int_{\mathbf{R}^*\times\prod_{p\leqslant X} C_p(-k,k)\times\prod_{p>X} \mathbf{Z}_p^*} |\phi(x)| d^*x.$$

然而 $\phi(x) = \prod_{v\in\mathscr{V}} \phi_v(x_v)$, 这让我们在 X 充分大时可将上式右端取成

$$(\int_{\mathbf{R}^*} |\phi_\infty(x_\infty)| d^*x_\infty) \prod_{p\leqslant X} (\int_{C_p(-k.k)} |\phi_p(x_p)| d^*x_p),$$

因为这时对所有的 $p > X$, 在 $\mathbf{Z}_p^*$ 上有 $\phi_p = 1$. 将 k 趋向 $+\infty$, 于是得到

$$\sum_{\beta\in I(X)} \int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*} |\phi(x)| d^*x = (\int_{\mathbf{R}^*} |\phi_\infty(x_\infty)| d^*x_\infty) \prod_{p\leqslant X} (\int_{\mathbf{Q}_p^*} |\phi_p(x_p)| d^*x_p),$$

现在让 X 趋向 $+\infty$ 便得到

$$\sum_{\beta\in\mathbf{Q}_+^*} \int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*} |\phi(x)| d^*x = \prod_{v\in\mathscr{V}} (\int_{\mathbf{Q}_v^*} |\phi(x_v)| d^*x_v) < +\infty,$$

从而 ϕ 可和. 特别地, 级数 $\sum_{\beta\in\mathbf{Q}^*}\int_{\beta\mathbf{R}_+^*\widehat{\mathbf{Z}}^*}\phi(x)d^*x$ 是绝对收敛的. 这让我们可以在上面的计算中去掉绝对值符号, 从而证明了公式 $\int_{\mathbf{A}^*}\phi(x)d^*x=\prod_{v\in\mathscr{V}}(\int_{\mathbf{Q}_v^*}\phi_v(x_v)d^*x_v)$, 这正是我们想要得到的. □

3.3. $\mathbf{Q}_p$ 上的梅林变换

引理 G.2.11. — 如果 χ 是 $\mathbf{Q}_p^*$ 的一个连续线性特征标, 则存在 $n\in\mathbf{N}-\{0\}$ 使得在 $1+p^n\mathbf{Z}_p$ 上 $\chi=1$.

证明 由于 χ 连续, 故存在 $n>0$ 使得当 $|x-1|_p\leqslant p^{-n}$ 时有 $|\chi(x)-1|\leqslant 1/2$. 然而 $B(1,p^{-n})=1+p^{n_p}\mathbf{Z}_p$ 是 $\mathbf{Z}_p^*$ 的具有有限指数的子群 (它是 $1\in(\mathbf{Z}/p^n\mathbf{Z})^*$ 在自然投射 $\mathbf{Z}_p^*\to(\mathbf{Z}_p/p^n\mathbf{Z}_p)^*=(\mathbf{Z}/p^n\mathbf{Z})^*$ 下的逆像). 由于 χ 是个群态射, $1+p^n\mathbf{Z}_p$ 的像是 $\mathbf{C}^*$ 的一个包含了圆盘 $D(1,1/2)$ 的子群; 由此知这个像化为了 1, 即为所证. □

称 χ 是非分歧的是说在 $\mathbf{Z}_p^*$ 上 $\chi=1$. 如果 χ 分歧, 则以 $n(\chi)$ 为使得在 $1+p^n\mathbf{Z}_p$ 上 $\chi=1$ 的最小 n; 于是 $p^{n(\chi)}$ 是 χ 的导子.

如果 G 为群, 称一个线性特征标 $\chi:G\to\mathbf{C}^*$ 是酉的是说, 对于任意的 $g\in G$ 有 $|\chi(g)|=1$. 因此对任意的 $g\in G$ 有 $\chi(g^{-1})=\overline{\chi}(g)$.

命题 G.2.12. — 设 $\chi:\mathbf{Q}_p^*\to\mathbf{C}^*$ 是一个连续的酉线性特征标,

(i) 如果 $\phi\in\mathscr{S}(\mathbf{Q}_p)$, 若 $\mathrm{Re}(s)>0$, 则 $x\mapsto\phi(x)\chi(x)|x|_p^s\in\mathscr{L}(\mathbf{Q}_p^*)$.

如果 $\mathrm{Re}(s)>0$, 设 $M_p(\phi,\chi,s)=\int_{\mathbf{Q}_p^*}\phi(x)\chi(x)|x|_p^sd^*x$, 则称其为 ϕ 的梅林变换.

[542] (ii) 如果 χ 是非分歧的, 则 $M_p(\mathbf{1}_{\mathbf{Z}_p},\chi,s)=\frac{1}{1-\chi(p)p^{-s}}$, 如果 χ 是分歧的, 则 $M_p(\mathbf{1}_{\mathbf{Z}_p},\chi,s)=0$.

(iii) 一般地, 如果 χ 是分歧的, 则 $M_p(\phi,\chi,s)$ 是 p^s 和 p^{-s} 的一个多项式, 而如果 χ 是非分歧的, 则其具有 $\frac{\phi(0)}{1-\chi(p)p^{-s}}+R(s)$ 形式, 其中 $R(s)$ 是 p^s 和 p^{-s} 的一个多项式.

证明 将 ϕ 写成 $\phi(0)\mathbf{1}_{\mathbf{Z}_p}+\psi$ 的形式, 其中 $\psi\in\mathscr{L}_0(\mathbf{Q}_p^*)$. 于是存在 $n\in\mathbf{N}$ 使得 $\psi\chi$ 是 mod $p^n\mathbf{Z}_p$ 常值, 显然我们可以将它写成形如 $\sum_{a\in I}\lambda_a\mathbf{1}_{a+p^n\mathbf{Z}_P}$. 因此我们有 $M_p(\psi,\chi,s)=\sum_{a\in I}\lambda_a\frac{p^{1-n}}{p-1}|a|_p^{s-1}$, 而由于 $|a|_p\in p^{\mathbf{Z}}$, 这便证明了 $M_p(\psi,\chi,s)$ 是 p^s 和 p^{-s} 的多项式.

现在, 我们有 $\int_{p^n\mathbf{Z}_p^*}||x|_p^s|d^*x=p^{-n\mathrm{Re}(s)}$. 因此得到 $x\mapsto\mathbf{1}_{\mathbf{Z}_p}(x)\chi(x)|x|_p^s$ 当 $\mathrm{Re}(s)>0$ 时是可和的. 进而有

$$\begin{aligned}M_p(\mathbf{1}_{\mathbf{Z}_p},\chi,s)&=\sum_{n=0}^{+\infty}\int_{p^n\mathbf{Z}_p^*}\chi(x)|x|_p^sd^*x=\sum_{n=0}^{+\infty}\int_{\mathbf{Z}_p^*}\chi(p^nx)|p^nx|_p^sd^*x\\&=\sum_{n=0}^{+\infty}\chi(p)^np^{-ns}\int_{\mathbf{Z}_p^*}\chi(x)d^*x=\frac{1}{1-\chi(p)p^{-s}}\int_{\mathbf{Z}_p^*}\chi(x)d^*x,\end{aligned}$$

而结果由当在 $\mathbf{Z}_p^*$ 上 $\chi=1$ 时 $\int_{\mathbf{Z}_p^*}\chi(x)d^*x=1$ 和当 χ 在 $\mathbf{Z}_p^*$ 上非平凡时此积分为 0 得到; 后面的断言成立是因为它可通过有限群 $(\mathbf{Z}/p^{n(\chi)}\mathbf{Z})^*$ 分解, 这时一个有限群的

非平凡线性特征标的取值的和为 0(线性特征标的正交性). □

3.4. 阿代尔上的梅林变换

命题 G.2.13. — 设 χ 是 $\mathbf{A}^*$ 的一个连续特征标, 如果 $v \in \mathscr{V}$, 那么设 χ_v 为 χ 在 $\mathbf{Q}_v^*$ 上的限制. 于是, 对几乎所有的 $p \in \mathscr{P}$, 我们在 $\mathbf{Z}_p^*$ 上有 $\chi_p = 1$, 而如果 $x \in \mathbf{A}^*$, 则 $\chi(x) = \prod_{v\in\mathscr{V}} \chi_v(x_v)$.

证明 由于 χ 在 $\mathbf{A}^*$ 上连续, 故在 $\widehat{\mathbf{Z}}^* = \prod_{p\in\mathscr{P}} \mathbf{Z}_p^*$ 上连续, 并由乘积拓扑的定义知, 存在有限集 $S \subset \mathscr{P}$, 若 $p \in S, n_p \in \mathbf{N} - \{0\}$, 则当 $x \in U = \prod_{p\in S}(1 + p^{n_p}\mathbf{Z}_p)\prod_{p\notin S} \mathbf{Z}_p^*$ 时, 有 $|\chi(x) - 1| \leqslant 1/2$. 然而 U 是 $\widehat{\mathbf{Z}}^*$ 的一个子群, 从而它在 χ 下的像是 $\mathbf{C}^*$ 的一个包含在圆盘 $D(1, 1/2)$ 中的子群; 由此推出这个像化为了 $\{1\}$. 特别地, 对于每个 $p \notin S$, 在 $\mathbf{Z}_p^*$ 上有 $\chi_p = 1$.

现在, 如果 $x \in \mathbf{A}^*$, 则对几乎所有的 v 有 $\chi_v(x_v) = 1$, 这让 $\chi'(x) = \prod_{v\in\mathscr{V}} \chi_v(x_v)$ 确有定义. 从而 χ' 是 $\mathbf{A}^*$ 的一个连续的线性特征标. 最后注意到 χ' 和 χ 在伊代尔的几乎所有分量等于 1 的子群上相同, 再利用这个子群在 $\mathbf{A}^*$ 中稠密便得到结果 (设 U 是 $\mathbf{A}^*$ 的一个开集, 如果它包含了 $\prod_{v\in S} U_v \times \prod_{p\notin S} \mathbf{Z}_p^*$, 则也包含了那些在 S 外的分量为 1 的元). □

如果 $\phi \in \mathscr{L}(\mathbf{R}^*)$, 而 χ 是 $\mathbf{R}^*$ 的一个连续线性特征标, ϕ 的一个梅林变换 $M_\infty(\phi, \chi, s)$ 是函数 $s \mapsto \int_{\mathbf{R}^*} \phi(t)\chi(t)|t|^s d^*t$, 如在定理 V.5.7 所证明的那样, 它在半平面 $\mathrm{Re}(s) > 0$ 上全纯.

命题 G.2.14. — 如果 χ 是 $\mathbf{A}^*$ 的一个连续的酉特征标, $v \in \mathscr{V}$, 设 χ_v 是 χ 在 $\mathbf{Q}_v^*$ 上的限制.

(i) 如果 $\phi \in \mathscr{S}(\mathbf{A})$, 则当 $\mathrm{Re}(s) > 1$ 时有 $x \mapsto \phi(x)\chi(x)|x|_{\mathbf{A}}^s \in \mathscr{L}(\mathbf{A}^*)$.

(ii) ϕ 的梅林变换 $M_{\mathbf{A}}(\phi, \chi, s) = \int_{\mathbf{A}^*} \phi(x)\chi(x)|x|_{\mathbf{A}}^s d^*x$ 在半平面 $\mathrm{Re}(s) > 1$ 上全纯.

(iii) 如果 $\phi = \otimes_{v\in\mathscr{V}}\phi_v$, 且若 $\mathrm{Re}(s) > 1$, 则 $M_{\mathbf{A}}(\phi, \chi, s) = \prod_{v\in\mathscr{V}} M_v(\phi_v, \chi_v, s)$. [543]

证明 先假设 $\phi = \otimes_{v\in\mathscr{V}}\phi_v$, 其中 $\phi_v \in \mathscr{S}(\mathbf{Q}_v)$, 且对几乎所有的 p 有 $\phi_p = 1_{\mathbf{Z}_p}$. 设 $\psi_v = \phi_v\chi_v|x_v|^s$. 由命题 G.2.12 得知, 当 $\mathrm{Re}(s) > 0$ 时, 对于任意的 $v \in \mathscr{V}$ 有 $\psi_v \in \mathscr{L}(\mathbf{Q}_v)$, 并且对几乎所有的 p 有 $\int_{\mathbf{Q}_p^*} |\psi_p| d^*x_p = \frac{1}{1-p^{-\mathrm{Re}(s)}}$. 由于 $\frac{1}{1-p^{-\mathrm{Re}(s)}}$ 对于 $\mathrm{Re}(s) > 1$ 收敛, 并由于在 $\mathbf{Z}_p^*$ 上对几乎所有的 p 有 $\psi_p = 1$, 故根据命题 G.2.13, 它满足命题 G.2.10 的映射条件. 由此得到 $\prod_{v\in\mathscr{V}} \psi_v = \phi(x)\chi(x)|x|_{\mathbf{A}}^s \in \mathscr{L}(\mathbf{A}^*)$, 其中 $\mathrm{Re}(s) > 1$, 从而

$$M_{\mathbf{A}}(\phi, \chi, s) = \prod_{v\in\mathscr{V}} \int_{\mathbf{Q}_v^*} \psi_v(x_v) d^*x_v = \prod_{v\in\mathscr{V}} M_v(\phi_v, \chi_v, s).$$

因为每个 $M_v(\phi_v, \chi_v, s)$ 在 $\mathrm{Re}(s) > 0$ 上全纯, 并且此乘积在整个上半平面 $\mathrm{Re}(s) > c$ $(c > 1)$ 上绝对收敛, 那么由此推出了 (定理 V.5.4) $M_{\mathbf{A}}(\phi, \chi, s)$ 在半平面 $\mathrm{Re}(s) > 1$

上的全纯性. 于是完成了对于 ϕ 是一个乘积的特殊情形的证明. (i) 和 (ii) 的一般情形则由线性性推出. □

3.5. 泰特 (Tate) 定理

下面的泰特定理让我们能够解析延拓阿代尔函数的梅林变换. 其证明基于阿代尔的泊松公式, 并对习题 VII.6.6 中为了解析延拓黎曼 ζ 函数时使用的方法做了极大的推广.

设 χ 是 $\mathbf{A}^*$ 的一个连续的酉特征标, 并设对于 $v \in \mathscr{V}$, χ_v 为 χ 在 $\mathbf{Q}_v^*$ 上的限制. 令 $S(\chi)$ 是那些使得 χ_p 为分歧的 p 的集合. 根据上面的命题 G.2.13 , 这个集合为有限集. 定义 χ 的导子 $D(\chi)$ 为 $D(\chi) = \prod_{p\in S(\chi)} p^{n(\chi_p)}$.

另外, χ_∞ 在 $\mathbf{R}_+^*$ 上的限制是个连续的酉特征标; 因此存在 $t(\chi) \in \mathbf{R}$ 使得 $\chi_\infty(x) = x^{it(\chi)}$, 其中 $x \in \mathbf{R}_+^*$.

定理 G.2.15. — (泰特, 1950) 如果 $\phi \in \mathscr{S}(\mathbf{A})$, 而 $\chi : \mathbf{A}^* \to \mathbf{C}^*$ 是一个在 $\mathbf{Q}^*$ 上平凡的连续酉特征标, 则 $M_{\mathbf{A}}(\phi, \chi, s)$ 具有到整个 $\mathbf{C}$ 上的亚纯延拓, 它在 $s = -it(\chi)$ 以及当 $D(\chi) = 1$ 时的 $s = 1 - it(\chi)$ 为单极点, 并在这些单极点外全纯, 而在这两个极点的留数分别为 $-\phi(0)$ 和 $\hat{\phi}(0)$, 并满足函数方程 $M_{\mathbf{A}}(\phi, \chi, s) = M_{\mathbf{A}}(\hat{\phi}, \overline{\chi}, 1-s)$.

证明 如果 $\mathrm{Re}(s) > 1$, 则有

$$M_{\mathbf{A}}(\phi, \chi, s) = \int_{\mathbf{A}^*} \phi(x)\chi(x)|x|_{\mathbf{A}}^s d^*x = \sum_{\beta\in\mathbf{Q}^*} \int_{\beta\mathbf{R}_+^* \widehat{\mathbf{Z}}^*} \phi(x)\chi(x)|x|_{\mathbf{A}}^s d^*x.$$

但 d^*x 和 $\chi(x)|x|_{\mathbf{A}}^s$ 在 $x \mapsto \beta x$ 下不变, 于是可以将前面的表达式重写为形如

$$\sum_{\beta\in\mathbf{Q}^*} \int_0^{+\infty} \int_{\widehat{\mathbf{Z}}^*} \phi(\beta x)\chi(x)|x|_{\mathbf{A}}^s d^*x = \int_0^{+\infty} \int_{\widehat{\mathbf{Z}}^*} \left(\sum_{\beta\in\mathbf{Q}^*} \phi(\beta x)\right) \chi(x)|x|_{\mathbf{A}}^s d^*x,$$

交换 $\sum$ 和 $\int$ 的合理性来自 $\phi(x)\chi(x)|x|_{\mathbf{A}}^s$ 在 $\mathbf{A}^*$ 上的可和性质.

[544] 现在, 由于 $\mathbf{Q}^* = \mathbf{Q} - \{0\}$, 阿代尔泊松公式 (定理 G.2.9) 可以将 $\sum_{\beta\in\mathbf{Q}^*} \phi(\beta x)$ 重写为形如

$$-\phi(0) + \sum_{\beta\in\mathbf{Q}} \phi(\beta x) = -\phi(0) + |x|_{\mathbf{A}}^{-1} \sum_{\beta\in\mathbf{Q}} \hat{\phi}(\beta x^{-1}) = \hat{\phi}(0)|x|_{\mathbf{A}}^{-1} - \phi(0) + |x|_{\mathbf{A}}^{-1} \sum_{\beta\in\mathbf{Q}^*} \hat{\phi}(\beta x^{-1}).$$

于是可以将积分 $\int_0^{+\infty}$ 分成 $\int_0^1 + \int_1^{+\infty}$, 并将 $\sum_{\beta\in\mathbf{Q}^*} \phi(\beta x)$ 换成在 $\int_0^1$ 中的表达式, 再在 $\int_0^1$ 中做变量变换 $x \mapsto x^{-1}$, 并利用恒等式 $\chi(x^{-1}) = \overline{\chi}(x)$(因为 χ 是酉的). 由于

$$\int_0^1 \int_{\widehat{\mathbf{Z}}^*} |x|_{\mathbf{A}}^u \chi(x) d^*x = (\int_0^1 x_\infty^{u+it(\chi)} \frac{dx_\infty}{x_\infty})(\prod_{p\in\mathscr{P}} \int_{\mathbf{Z}_p^*} \chi_p(x_p) d^*x_p)$$

$$= \begin{cases} 0, & \text{如果 } D(\chi) \neq 1, \\ \frac{1}{u+it(\chi)}, & \text{如果 } D(\chi) = 1 \end{cases}$$

(如果 $p \mid D(\chi)$, 则 $\int_{\mathbf{Z}_p^*} \chi_p(x_p) d^* x_p = 0$), 我们于是得到, 当 $D(\chi) \neq 1$ 时有

$$M_{\mathbf{A}}(\phi, \chi, s) = \int_1^{+\infty} \int_{\hat{\mathbf{Z}}^*} \sum_{\beta \in \mathbf{Q}^*} (\phi(\beta x)\chi(x)|x|_{\mathbf{A}}^s + \hat{\phi}(\beta x)\overline{\chi}(x)|x|_{\mathbf{A}}^{1-s}) d^* x,$$

而如果 $D(\chi) = 1$, 则应在上面添加 $-\frac{\phi(0)}{s+it(\chi)} - \frac{\hat{\phi}(0)}{1-s-it(\chi)}$. 因为对于所有 s 的值 $\sum_{\beta \in \mathbf{Q}^*} (\phi(\beta x)\chi(x)|x|^s + \bar{\phi}(\beta x)\overline{\chi}(x)|x|^{1-s})$ 是可和的, 从而定义了在整个 $\mathbf{C}$ 上的一个 s 的全纯函数; 又由公式 $\hat{\hat{\phi}}(x) = \phi(-x)$ 知道, 如果同时将 ϕ 换作 $\hat{\phi}$, χ 换作 $\overline{\chi}$ 以及 s 换作 $1-s$(我们还有 $t(\overline{\chi}) = -t(\chi)$) 证明, 这并没有改变所得结果. □

4. 对狄利克雷 L 函数的应用

定理 G.2.15 让我们可以重新证明狄利克雷 L 函数的解析延拓和函数方程的存在性. 但就所涉及的狄利克雷 L 函数而言, 并没有增加多少东西, 倒是对于赫克 L 函数而言, 阿代尔的计算就不再复杂了, 在这种情形, 相较于赫克原来的方法而言, 其改进是极其可观的.

4.1. 黎曼 ζ 函数

下面的结果已经证明过了, 而下面所给出的证明只不过是习题 VII.6.6 的证明的阿代尔翻版.

命题 G.2.16. — 设 $\xi(s) = \frac{\Gamma(s/2)}{\pi^{s/2}}\zeta(s)$. 则 $\xi(s)$ 有一个到 $\mathbf{C}$ 的亚纯延拓, 它在 $s=0$ 和 $s=1$ 的简单极点外全纯, 且在这两个简单极点的留数分别是 -1 和 1, 并满足函数方程 $\xi(1-s) = \xi(s)$.

证明 设 $\phi = \otimes_v \phi_v \in \mathscr{S}(\mathbf{A})$, 其中 $\phi_\infty(t) = e^{-\pi t^2}$, 而对任意的 $p \in \mathbf{Z}_p$, $\phi_p = \mathbf{1}_{\mathbf{Z}_p}$. 于是对任意的 v 有 $\hat{\phi}_v = \phi_v$, 从而 $\hat{\phi} = \phi$. 又, $\phi(0) = \hat{\phi}(0) = 1$. 由定理 G.2.15 得到 $M_{\mathbf{A}}(\phi, \mathbf{1}, s)$ 有到 $\mathbf{C}$ 的一个亚纯延拓, 它在 $s=0$ 和 $s=1$ 有简单极点, 其留数分别为 -1 和 1, 并满足函数方程 $M_{\mathbf{A}}(\phi, \mathbf{1}, 1-s) = M_{\mathbf{A}}(\phi, \mathbf{1}, s)$.

另外, 根据命题 G.2.14 的 (iii), 当 $\mathrm{Re}(s) > 1$ 时我们有 [545]

$$M_{\mathbf{A}}(\phi, \mathbf{1}, s) = \prod_{v \in \mathscr{V}} M_v(\phi_v, \mathbf{1}, s).$$

但如果 $p \in \mathscr{P}$, 那么根据命题 G.2.12 的 (ii) 有 $M_p(\phi_p, \mathbf{1}, s) = \frac{1}{1-p^{-s}}$, 因此

$$\prod_{p \in \mathscr{P}} M_p(\phi_p, \mathbf{1}, p) = \zeta(s).$$

最后,

$$M_\infty(\phi_\infty, \mathbf{1}, s) = M_\infty(e^{-\pi t^2}, \mathbf{1}, s) = \int_{\mathbf{R}^*} e^{-\pi t^2} t^s \frac{dt}{|t|} = \int_0^{+\infty} e^{-\pi u} u^{s/2} \frac{du}{u} = \frac{\Gamma(s/2)}{\pi^{s/2}}.$$

由此得到 $\xi(s) = M_{\mathbf{A}}(\phi, \mathbf{1}, s)$. 于是得到结论. □

4.2. $\mathbf{A}^*$ 的特征标的 L 函数

设 χ 是 $\mathbf{A}^*$ 的一个连续的酉线性特征标, 它在 $\mathbf{Q}^*$ 上平凡, 且其导子 $D(\chi)$ 不为 1, 又设 χ_v 是 χ 在 $\mathbf{Q}_v^*$ 上的限制, 其中 $v \in \mathscr{V}$.

由于 χ 是酉特征标, 故有 $\chi_\infty(x_\infty) = |x_\infty|^{it(\chi)}$ 或者 $\chi_\infty(x_\infty) = \mathrm{sign}(x_\infty)|x_\infty|^{it(\chi)}$. 在第一种情形, 称 χ 是偶的, 而第二种情形称其为奇的. 令

$$w_\infty(\chi) = \begin{cases} 1, & \chi \text{ 为偶的}, \\ -i, & \chi \text{ 为奇的}, \end{cases} \quad c(\chi) = \begin{cases} 0, & \chi \text{ 为偶的}, \\ 1, & \chi \text{ 为奇的}. \end{cases}$$

定义 $\varepsilon(\chi, s)$ 为 $\varepsilon(\chi, s) = \prod_v \varepsilon_v(\chi, s)$, 其中

$$\varepsilon_v(\chi, s) = \begin{cases} w_\infty(\chi), & \text{如果 } v = \infty, \\ w_p(\chi) p^{-n(\chi_p)s}, & \text{如果 } p \in \mathscr{P}, \end{cases}$$

其中

$$w_p(\chi) = \begin{cases} 1, & \text{如果 } p \nmid D(\chi), \\ \chi_p(p^{n(\chi_p)}) G(\overline{\chi}_p), & \text{如果 } p \mid D(\chi). \end{cases}$$

因此我们有 $\varepsilon(\chi, s) = (\prod_v w_v(\chi)) D(\chi)^{-s}$. (高斯和 $G(\overline{\chi}_p)$ 是利用同构 $(\mathbf{Z}_p/p^{n(\chi_p)}\mathbf{Z}_p)^* \cong (\mathbf{Z}/p^{n(\chi_p)}\mathbf{Z})^*$ 得到的导子 $p^{n(\chi_p)}$ 的狄利克雷特征标的高斯和.)

最后, 当 $\mathrm{Re}(s) > 1$ 时定义 χ 的 L 函数为 $L(\chi, s) = \prod_{p \nmid D(\chi)} \frac{1}{1 - \chi_p(p) p^{-s}}$.

命题 G.2.17. — 函数 $\Lambda(\chi, s) = \frac{\Gamma((s+it(\chi)+c(\chi))/2)}{\pi^{(s+it(\chi)+c(\chi))/2}} L(\chi, s)$ 有到 $\mathbf{C}$ 的一个全纯延拓, 并满足函数方程 $\Lambda(\chi, s) = \varepsilon(\chi, s)\Lambda(\overline{\chi}, 1-s)$.

证明　设 $\phi = \otimes_v \phi_v$, 其中

- 如果 χ 为偶的, 则令 $\phi_\infty(x) = e^{-\pi t^2}$, 如果 χ 为奇的, 则令 $\phi_\infty(x) = te^{-\pi t^2}$,
- 如果 $p \nmid D(\chi)$, 则令 $\phi_p = \mathbf{1}_{\mathbf{Z}_p}$,
- 如果 $p \mid D(\chi)$, 则令 $\phi_p = \mathbf{1}_{\mathbf{Z}_p^*} \overline{\chi}_p$.

我们对每个 v 来计算因子 $M_v(\phi_v, \chi_v, s)$ 和 $M_v(\hat{\phi}_v, \overline{\chi}_v, 1-s)$.

- 有 $\hat{\phi}_\infty = w_\infty(\chi)\phi_\infty$. 事实上, 如果 χ 是偶的, 这等价于说 $e^{-\pi t^2}$ 的傅里叶变换是 $e^{-\pi x^2}$. 如果 χ 是奇的, 这等价于说 $te^{-\pi t^2}$ 的傅里叶变换是 $-ixe^{-\pi x^2}$, 只要注意到 $-2\pi te^{-\pi t^2}$ 是 $e^{-\pi t^2}$ 的导数, 从而它的导数是 $e^{-\pi t^2}$ 的傅里叶变换的 $2i\pi x$ 倍, 则上述断言便可证明. 因此只要像确定 $M_\infty(e^{-\pi t^2}, \mathbf{1}, s)$ 曾经做过的那样, 稍加计算便得到

$$M_\infty(\phi_\infty, \chi_\infty, s) = \frac{\Gamma((s+it(\chi)+c(\chi))/2)}{\pi^{(s+it(\chi)+c(\chi))/2}}$$

和

$$M_\infty(\hat{\phi}_\infty, \overline{\chi}_\infty, s) = w_\infty(\chi)\frac{\Gamma((s+it(\chi)+c(\chi))/2)}{\pi^{(s+it(\chi)+c(\chi))/2}}.$$

- 如果 $p \nmid D(\chi)$, 则有 $\hat{\phi}_p = \mathbf{1}_{\mathbf{Z}_p}$, 从而, 根据命题 G.2.12 的 (ii), 如果 $\mathrm{Re}(s) > 0$, 则 [546]

$$M_p(\phi_p, \chi_p, s) = \frac{1}{1 - \chi_p(p)p^{-s}} \quad 和 \quad M_p(\hat{\phi}_p, \overline{\chi}_p, s) = \frac{1}{1 - \overline{\chi}_p(p)p^{-s}}.$$

- 如果 $p \mid D(\chi)$, 则直接的计算可证明有 $M_p(\phi_p, \chi_p, s) = 1$. 另外, 根据习题 G.2.7 的 (iii) 有 $\hat{\phi}_p(x) = \frac{G(\overline{\chi}_p)}{p^{n(\chi_p)}} \chi_p(p^{n(\chi_p)}x)\mathbf{1}_{p^{-n(\chi_p)}\mathbf{Z}_p^*}(x)$, 因此

$$\begin{aligned} M_p(\hat{\phi}_p, \overline{\chi}_p, 1-s) &= \frac{G(\overline{\chi}_p)}{p^{n(\chi_p)}} \int_{p^{-n(\chi_p)}\mathbf{Z}_p^*} \chi_p(p^{n(\chi_p)}x)\overline{\chi}_p(x)|x|_p^{1-s} d^*x \\ &= \frac{G(\overline{\chi}_p)}{p^{n(\chi_p)}} \chi_p(p^{n(\chi_p)}) p^{n(\chi_p)(1-s)} \int_{p^{-n(\chi_p)}\mathbf{Z}_p^*} d^*x = w_p(\chi)p^{-n(\chi_p)(s)}. \end{aligned}$$

因此, 当 $\mathrm{Re}(s) > 1$ 时有

$$\begin{aligned} M_{\mathbf{A}}(\phi, \chi, s) &= \prod_{v \in \mathscr{V}} M_v(\phi_v, \chi_v, s) \\ &= \frac{\Gamma((s + it(\chi) + c(\chi))/2)}{\pi^{(s+it(\chi)+c(\chi))/2}} \prod_{p \nmid D(\chi)} \frac{1}{1 - \chi_p(p)p^{-s}} = \Lambda(\chi, s). \end{aligned}$$

同样地, 如果 $\mathrm{Re}(s) < 0$, 则 $M_{\mathbf{A}}(\hat{\phi}, \overline{\chi}, 1-s) = \prod_{v \in \mathscr{V}} M_v(\hat{\phi}_v, \overline{\chi}_v, 1-s)$ 也等于

$$w_\infty(\chi) \frac{\Gamma((1 - s + it(\chi) + c(\chi))/2)}{\pi^{(1-s+it(\chi)+c(\chi))/2}} \Big(\prod_{p \mid D(\chi)} w_p(\chi) p^{-n(\chi_p)(s)} \Big) \prod_{p \nmid D(\chi)} \frac{1}{1 - \overline{\chi}_p(p)p^{-(1-s)}},$$

就是说等于 $\varepsilon(\chi, s)\Lambda(\overline{\chi}, 1-s)$. 因此结论由定理 G.2.15 并利用如下事实得到: 如果 $p \mid D(\chi)$, 因为 $\phi_p(0) = \hat{\phi}_p(0) = 0$ 有 $\phi(0) = \hat{\phi}(0) = 0$. □

4.3. 狄利克雷特征标和伊代尔的连续线性特征标

按照引理 G.2.5, 我们可以对于一个导子为 D 的狄利克雷特征标 χ 伴以一个 $\mathbf{A}^*$ 的有限阶的连续线性特征标 $\chi_{\mathbf{A}}$(从而是酉的), 它由公式 $\chi_{\mathbf{A}}(x) = \chi(\pi_D(b^{]\infty[}))^{-1}$ 给出, 其中 $x = \beta b_\infty b^{]\infty[}$, 而 $\beta \in \mathbf{Q}^*, b_\infty \in \mathbf{R}_+^*, b^{]\infty[} \in \widehat{\mathbf{Z}}^*$, 并且 $\pi_D : \widehat{\mathbf{Z}}^* \to (\mathbf{Z}/D\mathbf{Z})^*$ 为自然投射[36]. 注意, 由构造知 $\chi_{\mathbf{A}}$ 在 $\mathbf{Q}^*$ 上平凡.

引理 G.2.18. — $L(\chi_{\mathbf{A}}, s) = L(\chi, s)$.

证明 以 χ_p 记 $\chi_{\mathbf{A}}$ 在 $\mathbf{Q}_p^*$ 上的限制, 那么问题是要证明如果 $p \nmid D$, 则 $\chi(p) = \chi_p(p)$. 设 x(分别地, y) 是除了在 p 的分量等于 p(分别地, 1), 其余的分量全为 1(分别地, p^{-1}) 的伊代尔. 于是由定义有 $\chi_p(p) = \chi_{\mathbf{A}}(x)$, 并且由于 $x = py$, 故 $\chi_p(p) = \chi(\pi_D(y^{]\infty[}))^{-1}$. 但 $y^{]\infty[}$ 在 ℓ 整除 D 的所有那些分量等于 p^{-1}; 由此得到 $\pi_D(y^{]\infty[}) = p^{-1}$, 故 $\chi_p(p) = \chi(p^{-1})^{-1} = \chi(p)$. 得到了结论. □

从这个引理和命题 G.2.17 得到了 $L(\chi, s)$ 的解析延拓和函数方程的存在性. 除此以外, 这个引理也让我们将克罗内克–韦伯定理重新写为如下形式. [547]

[36] 如果 $p \nmid D$, 它将 $\mathbf{Z}_p^*$ 映成 1, 而当 $p \mid D$ 时, $\mathbf{Z}_p^*$ 则映到 $(\mathbf{Z}_p/p^{v_p(D)}\mathbf{Z}_p)^* = (\mathbf{Z}/p^{v_p(D)}\mathbf{Z})^*$ 上, 并利用由中国剩余定理给出的同构 $(\mathbf{Z}/D\mathbf{Z})^* = \prod_{p \mid D}(\mathbf{Z}/p^{v_p(D)}\mathbf{Z})^*$.

定理 G.2.19. — 如果 ρ 是 $\mathscr{G}_{\mathbf{Q}}$ 的一个一维表示, 则存在 $\mathbf{A}^* = \mathbf{GL}_1(\mathbf{A})$ 的在 $\mathbf{Q}^* = \mathbf{GL}_1(\mathbf{Q})$ 为平凡的连续的酉线性特征标 $\chi(\rho)$, 使得 $L(\rho, s) = L(\chi(\rho), s)$.

G.3. 朗兰兹纲领

朗兰兹纲领是将上面定理 G.2.19 的陈述中的 1 换作 n(说易做难 $\cdots\cdots$).

1. 自守表示

以 G 记群 $\mathbf{GL}_n$, 于是 $G(\mathbf{A}), G(\mathbf{Q}), G(\mathbf{R}), G(\mathbf{Q}_p)$ 和 $G(\mathbf{Z}_p)$ 分别代表了群 $\mathbf{GL}_n(\mathbf{A})$, $\mathbf{GL}_n(\mathbf{Q}), \mathbf{GL}_n(\mathbf{R}), \mathbf{GL}_n(\mathbf{Q}_p)$ 和 $\mathbf{GL}_n(\mathbf{Z}_p)$. 故而 $G(\mathbf{A})$ 是 $G(\mathbf{Q}_v)$ 相对于 $G(\mathbf{Z}_p)$ 的限制乘积, 其中 $v \in \mathscr{V}$, $p \in \mathscr{P}$. 换句话说, $G(\mathbf{A})$ 的元 x 形如 $(x_v)_{v\in\mathscr{V}}$, 其中 $x_v \in G(\mathbf{Q}_v)$ 而 $x_p \in G(\mathbf{Z}_p)$ 对几乎所有的 p 成立. 我们也将 x 写成 $(x_\infty, x^{]\infty[})$ 的形式, 其中 $x^{]\infty[} = (x_p)_{p\in\mathscr{P}}$ 是 x 在 ∞ 之外的部分. 按习惯, 将 $G(\mathbf{Q}_v)$ $(v \in \mathscr{V})$ 等同于 $G(\mathbf{A})$ 的一个子群.

设 $\mathscr{A}_0(G(\mathbf{Q}) \setminus G(\mathbf{A}))$ 是 $G(\mathbf{A})$ 的尖点自守形式的 $\mathbf{C}$-向量空间[37], 就是说, 是那些满足以下条件的函数 $\phi : G(\mathbf{A}) \to \mathbf{C}$ 的空间:

(i) 对任意的 $\gamma \in G(\mathbf{Q})$ 和 $x \in G(\mathbf{A})$ 有 $\phi(\gamma x) = \phi(x)$;

(ii) 在 $\prod_{p\in\mathscr{P}} G(\mathbf{Z}_p)$ 中存在一个有限指标的 K_ϕ 使得对任意的 $x \in G(\mathbf{A})$ 和 $h \in K_\phi$ 有 $\phi(xh) = \phi(x)$, 并且对于 $h \in \mathbf{O}_n(\mathbf{R})$, 这些 $\phi(xh)$ 生成了一个有限维的空间[38];

(iii) 存在 $\mathbf{A}^*$ 的一个在 $\mathbf{Q}^*$ 上平凡的连续酉线性特征标 χ, 使得 $\phi(A_z x) = \phi(xA_z) = \chi(z)\phi(x)$, 其中 A_z 是比率为 $z \in \mathbf{A}^*$ 的位似变换的矩阵;

(iv) 如果 $x^{]\infty[}$ 固定不动, 则 $\phi(x_\infty, x^{]\infty[})$ 是 x_∞ 的坐标的 $\mathscr{C}^\infty$ 类函数;

(v) ϕ 在无限远速降 (我们不准备给出其准确意思).

给出 $g \in G(\mathbf{A})$ 在函数 $\phi : G(\mathbf{A}) \to \mathbf{C}$ 上的作用为对变量的右平移, 这就是说, [548] $g \cdot \phi(x) = \phi(xg)$. 空间 $\mathscr{A}_0(G(\mathbf{Q}) \setminus G(\mathbf{A}))$ 在 $G(\mathbf{A})$ 的作用下是不稳定的, 但却几乎是稳定的[39], 而我们假装它是 (脚注 39 给出了正确的陈述). 因此 $\mathscr{A}_0(G(\mathbf{Q}) \setminus G(\mathbf{A}))$ 是

---

[37] "自守" 等于是 (i), 这是 (i)—(v) 中最精妙的部分, 而 "尖点" 则对应了条件 (v).

[38] 群 $\mathbf{O}_n(\mathbf{R})$ 是 $\mathbf{R}^n$ 的等距变换群; 这是 $G(\mathbf{R})$ 的一个紧子群, 它是具有这个性质的最大子群, 同样地, $G(\mathbf{Z}_p)$ 是 $G(\mathbf{Q}_p)$ 的一个紧子群并是具有此性质的最大者.

[39] 它在 $G(\mathbf{A}^{]\infty[}), \mathbf{O}_n(\mathbf{R})$ 作用下稳定, 而因为条件 (iii) 需要 $\phi(xh)$ $(h \in \mathbf{O}_n(\mathbf{R}))$ 生成一个有限维的空间. 相反地, 在 $G(\mathbf{R})$ 的无穷小作用下是稳定的, 这是说, 在微分算子 ∂_A 的作用下稳定, 其中 $A \in \mathbf{M}_n(\mathbf{R})$, 而 $\partial_A\phi(x) = \lim_{t\to 0} t^{-1}(\phi(xe^{tA}) - \phi(x))$, $e^{tA} = \sum_{n=0}^{+\infty} \frac{t^n A^n}{n!} \in G(\mathbf{R})$ 是矩阵 tA 的指数函数. 由于 $e^{tA} \in \mathbf{O}_n(\mathbf{R})$ 当 (且仅当)A 是反称的, 故 $\mathbf{O}_n(\mathbf{R})$ 和 $\mathbf{M}_n(\mathbf{R})$ 的作用有应该满足的显然的相容条件. 后面, 我们会不恰当地称呼 $G(\mathbf{R})$(分别地, $G(\mathbf{A})$) 的表示为一个具有 $\mathbf{O}_n(\mathbf{R})$ 和 $\mathbf{M}_n(\mathbf{R})$ 作用的 $\mathbf{C}$-向量空间, 实际应满足了上面提到的相容关系.

$G(\mathbf{A})$ 的一个表示. 于是 $\mathscr{A}_0(G(\mathbf{Q})\setminus G(\mathbf{A}))$ 可分解为不可约表示的直和 (它的不可约分支是所谓的尖点自守表示). 下面的定理展示了某些成果 (对于 $n=2$, 属于 Jacquet 和 Langlands(1969), 而对 $n\geqslant 3$ 的应归功于 Godement 和 Jacquet (1972)). 自守 L 函数的存在性和解析延拓性的证明则受到了泰特为了研究赫克 L 函数而引进的方法的强烈启发.

定理 G.3.1. — 设 Π 是 n 次尖点自守表示, 则

(i) Π 具有一个形如 $\Pi=\otimes'_{v\in\mathscr{V}}\Pi_v$ 的分解[40], 其中 Π_v 是 $G(\mathbf{Q}_v)$ 的一个 (无穷维的) 不可约表示.

(ii) Π 有一个可分解为形如 $L(\Pi,s)=\Pi_{v\in\mathscr{V}}L(\Pi_v,s)$ 的 L 函数[41], 其中 $L(\Pi_\infty,s)$ 是一个只依赖 Π_∞ 的 Γ 函数的乘积, 而 $L(\Pi_p,s)=\frac{1}{E_p(p^{-s})}$, 其中 $E_p(X)$ 是一个 $\leqslant n$ 次的多项式, 且对几乎所有的 p 这个次数等于 n, 其常数项为 1, 并只与 Π_p 有关.

(iii) $L(\Pi,s)$ 具有到整个复平面上的解析延拓, 并具有一个形如 $L(\Pi,s)=\varepsilon(s)L(\Pi^\vee,1-s)$ 的函数方程, 其中 $\Pi^\vee$ 是另一个尖点自守表示 (Π 的逆步表示), [549] $\varepsilon(s)$ 具有 $A\cdot B^s$ 的形式, 其中 $A\in\mathbf{C}^*, B\in\mathbf{R}_+^*$.

猜想 G.3.2. — (朗兰兹, 1968) 如果 ρ 是 $\mathscr{G}_\mathbf{Q}$ 的一个 n 维不可约表示, 则存在一个 n 次的尖点自守表示使得 $L(\rho,s)=L(\Pi(\rho),s)$.

鉴于上面的定理, 这个猜想蕴含了阿廷猜想, 但实际上还远不止此. 这不过只是朗兰兹猜想存在性大厦的一小块而已.

我们将在第二小节中证明如何把一个本原模形式或者一个本原 Maass 形式变换为 $\mathbf{GL}_2(\mathbf{A})$ 的一个尖点自守表示, 它让我们可以将尖点自守形式看成是本原模 (或 Maass) 形式的巨大推广. 我们留意到, 在 $\geqslant 3$ 次的情形似乎不一定有它与模形式或 Maass 形式之间的等价关系, 但是用表示论的语言却很难避免.

---

[40] 群 $G_\mathbf{A}$ 本质上是一个乘积. 但我们已经看到, 在有限群的情形, 如果 $G=G_1\times G_2$, 则 G 的每个不可约表示可分解为 $V_1\otimes V_2$, 其中 V_i 是 G_i 的不可约表示, 其中 $i=1,2$. 所以会自然地想到 $G_\mathbf{A}$ 的一个不可约表示也具有一个分解, 这就是定理 3.1 的 (i) 所断言的. 另一方面, 做无限多个向量空间的张量积却不太合理, 但定理中的张量积是一个限制的张量积. (我们已经见过这个概念的例子: $\mathscr{S}(\mathbf{A})$ 是 $\mathscr{S}(\mathbf{Q}_v)$ 对于 $v\in\mathscr{V}$ 的相对于函数 $\mathbf{1}_{\mathbf{Z}_p}$ ($p\in\mathscr{P}$) 的限制张量积; 同样, $\mathscr{L}_0(\mathbf{A}^*)$ 是 $\mathscr{L}(\mathbf{R}^*)$ 与 $\mathscr{L}_0(\mathbf{Q}_p^*)$ ($p\in\mathscr{P}$) 相对于函数 $\mathbf{1}_{\mathbf{Z}_p^*}$ ($p\in\mathscr{P}$) 的限制乘积.) 准确地说, 对于所有的 p 使得定理的 (ii) 中的多项式 E_p 的次数为 n, 于是表示 Π_p 具有一个被 $G(\mathbf{Z}_P)$ 固定的特定向量 x_p (被差一个 $\mathbf{C}^*$ 中的乘法因子确定, 但这个不确定性并不重要). 因此, 相对于向量 x_p 的限制张量积 $\otimes_{v\in\mathscr{V}}\Pi_v$ 由形如 $\otimes_{v\in\mathscr{V}}y_v$ 生成, 而其中对几乎所有的 p 满足 $y_p=x_p$. 我们需注意, $g\in G_\mathbf{A}$ 自然地以公式 $g\cdot(\otimes_{v\in\mathscr{V}}y_v)=\otimes_{v\in\mathscr{V}}(g_v\cdot y_v)$ 作用于这种类型的元, 这就像在两个群的表示的张量积的情形一样, 重要之处是对几乎所有的 p, $g_p\in G(\mathbf{Z}_p)$, 从而对几乎所有的 p 有 $g_p\cdot y_p=x_p$.

[41] 这些自守 L 函数大大推广了狄利克雷 L 函数.

2. 对自守表示的模形式

2.1. 一点准备

如果 $D \in \mathbf{N}$, 令 K^D 为 $\mathbf{GL}_2(\widehat{\mathbf{Z}}) = \prod_{p\in\mathscr{P}} \mathbf{GL}_2(\mathbf{Z}_p)$ 中的元 $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $(c \in D\widehat{\mathbf{Z}})$ 构成的子群. 如果 χ 是 mod D 的狄利克雷特征标, 定义 $\tilde{\chi}(h) = \chi(\bar{d})$, 其中 $\bar{d}$ 是 d 在 $(\widehat{\mathbf{Z}}/D\widehat{\mathbf{Z}})^* = (\mathbf{Z}/D\mathbf{Z})^*$ 中的像, 从而给出了 K^D 的一个线性特征标 $\tilde{\chi}$. 于是对于 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(D)$, 则 $\tilde{\chi}(\gamma) = \chi_0(D)$.

命题 G.3.3. — (i) $\mathbf{GL}_2(\mathbf{A})$ 的元可以写为形如 $\gamma g_\infty \kappa$ 的元, 其中 $\gamma \in \mathbf{GL}_2(\mathbf{Q}), g_\infty \in \mathbf{GL}_2(\mathbf{R})^+ = \{g \in \mathbf{GL}_2(\mathbf{R}), \det g > 0\}$, 而 $\kappa \in K^D$.

(ii) 这个写法形式唯一到相差 γ 的右乘 $\alpha \in \Gamma_0(D)$ 因子以及 g_∞ 和 κ 的左乘 α^{-1} 因子.

证明　参看 2.3 小节. □

2.2. 与一个模形式相伴的自守形式

设 $f \in S_k(D,\chi)$. 我们可以利用上面 $\mathbf{GL}_2(\mathbf{A})$ 的分解将 f 联系到一个 $\mathbf{GL}_2(\mathbf{A})$ 上的函数 ϕ_f, 其定义公式是

$$\phi_f(x) = \tilde{\chi}(h)^{-1}\left(\frac{(a_\infty d_\infty - b_\infty c_\infty)^{1/2}}{c_\infty i + d_\infty}\right)^k f\left(\frac{a_\infty i + b_\infty}{c_\infty i + d_\infty}\right),$$

其中

$$x = \gamma g_\infty h,\ g_\infty = \begin{pmatrix} a_\infty & b_\infty \\ c_\infty & d_\infty \end{pmatrix}.$$

命题 G.3.3 和 $(cz+d)^{-k} f(\frac{az+b}{cz+d}) = \chi(d) f(z)$, (其中 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(D)$) 这个性质证明了它不依赖 x 的分解的选取. 不太难便可证明 ϕ_f 是一个尖点自守形式.

[550] 对于一个特征标 χ, 特征值 λ 的对于 $\Gamma_0(D)$ 的 Maass 形式 f, 我们以同样的方法定义 ϕ_f, 其定义公式为 $\phi_f(x) = \tilde{\chi}(h)^{-1} f(g_\infty)$.

在这两种情形中, 都以 Π_f 记在 $\mathbf{GL}_2(\mathbf{A})$ 作用下由 ϕ_f 生成的 $\mathscr{A}_0(\mathbf{GL}_2(\mathbf{Q}) \backslash \mathbf{GL}_2(\mathbf{A}))$ 的子空间. 下面的定理可以看成是朗兰兹纲领的出发点.

定理 G.3.4. — 如果 f 是本原的, 则 Π_f 是个 2 次尖点自守表示, 因而具有形如 $\Pi_f = \otimes_{v\in\mathscr{V}} \Pi_{f,v}$ 的分解.

(ii) 如果 f 是 D 级的, 且如果 p 不整除 D, 则表示 $\Pi_{f,v}$ 可以完全由函数 $L(f,s)$ 在 p 的欧拉因子 $E_p(f,s)$ 描述, 并且 $L(\Pi_{f,p},s) = E_p(f,s)^{-1}$.

为了准确地阐述 (ii), 我们分解欧拉因子 $E_p(f,s)$ 如下:

$$\begin{cases} E_p(f,s+\frac{k-1}{2})=(1-\alpha_p p^{-s})(1-\beta_p p^{-s}), & \text{如果 } f \text{ 是一个权为 } k \text{ 的模形式}, \\ E_p(f,s)=(1-\alpha_p p^{-s})(1-\beta_p p^{-s}), & \text{如果 } f \text{ 是个 Maass 形式}. \end{cases}$$

由此可定义 $\mathbf{Q}_p^*$ 的两个特征标 μ_1,μ_2, 定义公式分别为 $\mu_1(x)=\alpha_p^{-v_p(x)}$ 和 $\mu_2(x)=\beta_p^{-v_p(x)}$. 因而表示 $\Pi_{f,p}$ 是以 $\mathbf{GL}_2(\mathbf{Q}_p)$ 作用得到的表示 $I(\mu_1,\mu_2)$, 这里的作用是对于在 $\mathbf{GL}_2(\mathbf{Q}_p)$ 上的局部常值函数空间 φ 的右平移, 使得

$$\phi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} x\right)=\mu_1(a)\mu_2(d)|\frac{a}{d}|^{1/2}\phi(x),$$

其中 $a,d\in\mathbf{Q}_p^*$, $b\in\mathbf{Q}_p$, $x\in\mathbf{GL}_2(\mathbf{Q}_p)$. 上面的构造不禁使人想起对有限群所诱导的表示的构造 (参看 C.3 的第 2 小节), 如果以 B 记 $\mathbf{GL}_2(\mathbf{Q}_p)$ 的博雷尔子群 (即上三角矩阵的子群), 那么 $I(\mu_1,\mu_2)$ 被诱导成了局部常值的 B 的线性表示 $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\mapsto\mu_1(a)\mu_2(d)|\frac{a}{b}|^{1/2}$ 的集合 G.

对表示 $\Pi_{f,p}$ $(p\mid D)$ 描述更加难以捉摸. 它的描述应归到局部朗兰兹对应的框架内.

2.3. $\mathbf{GL}_2(\mathbf{A})$ 的分解

引理 G.3.5. — 如果 S 是 $\mathscr{P}$ 的一个有限子集, 则 $\mathbf{SL}_2(\mathbf{Z}[S^{-1}])$ 在 $\prod_{p\in S}\mathbf{SL}_2(\mathbf{Q}_p)$ 中稠密.

证明 设 $A=(A_p)_{p\in S}\in\prod_{p\in S}\mathbf{SL}_2(\mathbf{Q}_p)$. 根据引理 B.2.2, 可以将 A_p 写成形如 $A_p=\begin{pmatrix} - & 0 \\ t_p & 1 \end{pmatrix}\begin{pmatrix} 1 & x_p \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ y_p & 1 \end{pmatrix}\begin{pmatrix} 1 & z_p \\ 0 & 1 \end{pmatrix}$, 其中 $t_p,x_p,y_p,z_p\in\mathbf{Q}_p$. 由于 $\mathbf{Z}[S^{-1}]$ 在 $\prod_{p\in S}\mathbf{Q}_p$ 中稠密, 故可找到在 $\mathbf{Z}[S^{-1}]$ 中的序列 $(t'_n)_{n\in\mathbf{N}},(x'_n)_{n\in\mathbf{N}},(y'_n)_{n\in\mathbf{N}}$ 和 $(z'_n)_{n\in\mathbf{N}}$ 对于所有 $p\in S$ 分别趋向 t_p,x_p,y_p 和 z_p. 如果令

$$A'_n=\begin{pmatrix} - & 0 \\ t'_n & 1 \end{pmatrix}\begin{pmatrix} 1 & x'_n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ y'_n & 1 \end{pmatrix}\begin{pmatrix} 1 & z'_n \\ 0 & 1 \end{pmatrix},$$

则 $(A'_n)_{n\in\mathbf{N}}$ 是 $\mathbf{SL}_2(\mathbf{Z}[S^{-1}])$ 中的序列, 它趋向 $\prod_{p\in S}\mathbf{SL}_2(\mathbf{Q}_p)$ 中的 A. 得证. □

下面继续命题 G.3.3 的证明. 设 $g\in\mathbf{GL}_2(\mathbf{A})$. 由于 $\det g\in\mathbf{A}^*$, 故可将 $\det g$ 以唯一的方式写成 βb 的形式, 其中 $b=(b_\infty,b^{]\infty[})$, 而 $\beta\in\mathbf{Q}^*,b_\infty\in\mathbf{R}_+^*$ 以及 $b^{]\infty[}\in\prod_{p\in\mathscr{P}}\mathbf{Z}_p^*$. 于是 $h=\begin{pmatrix} \beta^{-1} & 0 \\ 0 & 1 \end{pmatrix}g\begin{pmatrix} b^{-1} & 0 \\ 0 & 1 \end{pmatrix}\in\mathbf{SL}_2(\mathbf{A})$. 设 S 是 $\mathscr{P}$ 中 [551] 的整除 D 的 p 和那些使得 $h_p\notin\mathbf{SL}_2(\mathbf{Z}_p)$ 的 p 的集合. 根据引理 G.3.5, 可以找到 $\gamma_0\in\mathbf{SL}_2(\mathbf{Z}[S^{-1}])$ 使得其与 $(h_p)_{p\in S}$ 可随意地靠近; 特别地, 可找到 $\gamma_0\in\mathbf{SL}_2(\mathbf{Z}[S^{-1}])$ 使得 $\gamma_0^{-1}h_p=\begin{pmatrix} a_p & b_p \\ c_p & d_p \end{pmatrix}\in\mathbf{SL}_2(\mathbf{Z}_p)$, 其中 $p\in S$, 并且满足 $v_p(c_p)\geqslant v_p(D)$, 其

中 p 为整除 D 的任意素数. 因此 $\gamma = \begin{pmatrix}\beta & 0\\ 0 & 1\end{pmatrix}\gamma_0$, $g_\infty = \gamma_0^{-1}h_\infty\begin{pmatrix}b_\infty & 0\\ 0 & 1\end{pmatrix}$, 而 $\kappa = \gamma_0^{-1}h^{]\infty[}\begin{pmatrix}b^{]\infty[} & 0\\ 0 & 1\end{pmatrix}$ 给出了 g 的一个我们想要的分解. (i) 得证.

(ii) 完全来自以下事实, 即在 $\mathbf{GL}_2(\mathbf{Q})$ 与 $\mathbf{GL}_2(\mathbf{R})^+K^D$ 相交处的 $\gamma = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ 和它的逆的系数均在 $\mathbf{Z}$ 中, 行列式为正, 并满足对任意的 $p \in \mathscr{P}$ 有 $v_p(c) \geqslant v_p(D)$. 换言之, 它是 $\Gamma_0(D)$ 中的元.

3. 朗兰兹纲领的其他一些方面

朗兰兹纲领还有其他的许多方面. 特别地, 在我们讨论过的所有对象中都可将 $\mathbf{Q}$ 换作数域 F; 以同样的方法, 也可从 F 的所有完备化 F_v 出发去构造 F 的阿代尔环.

- *局部朗兰兹对应.* 它是在 $\mathscr{G}_{\mathbf{Q}_p}$ 的 n 维不可约表示与 $\mathbf{GL}_n(\mathbf{Q}_p)$ 的某些不可约表示 (尖点表示) 之间的一个对应关系. 这个对应最终在完全一般的情形下[42] 被 M. Harris (巴黎第七大学) 和 R. Taylor (哈佛大学) 在 1999 年建立起来了, 后由 G. Henniart (Orsay) 于 1999 年加以简化. 给出了对群 $\mathscr{G}_{\mathbf{Q}_p}$ 一个间接的但很有用的描述.

- *对于函数域的朗兰兹对应.* 固定一个素数 p. 代替 $\mathbf{Q}$ 和数域, 我们可以考虑系数在 $\mathbf{F}_p$ 中的有理分式域 $\mathbf{F}_p(X)$ 的有限扩域 K. K 的阿代尔环是从 $\mathbf{F}_p(X)$ 对在 $\mathbf{F}_p(X)$ 所取得不同的范数的完备化着手; 与数域的一个区别是, 这些完备化都很相像: 它们全具有 $\mathbf{F}_q((T))$ 的形式, 即系数在 $\mathbf{F}_q$ 中的形式级数环的有理分式域, 其中 $\mathbf{F}_q$ 是具有 q 个元的有限域而 q 是 p 的一个幂. 在这个架构下, 朗兰兹对应由拉福格 (L. Lafforgue) (I.H.E.S., Bures sur Yvette) 在 1999 年建立, 这为他赢得了菲尔兹奖 (2002). 在它的证明中用到了由格罗滕迪克在 20 世纪 60 年代引进的代数几何; $n = 2$ 的情形已由德林费尔德 (V. Drinfeld) 在 20 世纪 70 年代建立 (1990 年的菲尔兹奖), 而拉福格的证明是德林费尔德的证明的巨大推广.

- *朗兰兹纲领的函子性.* 鉴于伽罗瓦理论, 从已知的表示出发我们有许多构造方法去产生新的表示. 例如, 如果 $F \subset K$ 是两个数域, 且若 ρ 是 $\mathscr{G}_F$(分别地, $\mathscr{G}_K$) 的一个表示, 我们则可考虑 ρ 在 $\mathscr{G}_K$(分别地, $\mathscr{G}_F$) 的限制 (分别地, 诱导). 所有这些构造在自守 [552] 表示方面都有其类似, 但我们离真正理解仍很远, 即便在 2008 年吴宝珠 (现在在芝加哥大学) 取得了 "基本引理" 的证明依然如此; 这个 "基本引理" 是 20 多年前由朗兰兹和 D. Shelstad 提出来的 (称之为 "引理" 是因为它似乎像一个组合的小恒等式, 而称之为 "基本" 则是因为缺少了它的证明就会阻挡了向前推进的步伐), 为此吴宝珠得到了 2010 年的菲尔兹奖. 它的证明建立在由 M. Goreski, R. MacPherson, R. Kottwitz, G. Laumon 和 J.-L. Waldspurger (以及其他) 给出的理论和约化的十分深刻的架构之上.

---

[42]按同样的方法我们可以考虑用数域代替 $\mathbf{Q}$, 就可以考虑代替 $\mathbf{Q}_p$ 的数域的完备化 F_v.

- 几何朗兰兹纲领 (似乎美国军方对此有兴趣). 它并非最初的朗兰兹纲领的一部分: 这是围绕着 V. Drinfeld 和 A. Beilinson (现在两人都在芝加哥大学) 的俄罗斯学派拓展出来的, 其动机来自与弦论相关的数学物理, 涉及对于函数域的一个对应纲领, 在那里将有限域换成了复数域 $\mathbf{C}$.

附录 H. 问题校正

[553]

以下的习题和问题取自第 I—VII 章的内容.

— 习题 H.1.1, H.1.2, H.1.3 和问题 H.2, H.3, H.4 的目标是建立一个有限群的特征标表 (它们分别作用在 $S_3, S_4, \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\} \subset \mathbf{GL}_2(\mathbf{F}_q), A_5, \mathbf{GL}_2(\mathbf{F}_3)$ 以及 $\mathbf{GL}_3(\mathbf{F}_2)$ 上). 难度在逐渐增大, 但使用的技术在问题之间却是相似的; 上面的这三个问题则是为了对第 I 章的主要陈述进行复习而设计的.

— 问题 H.5 探索了连续函数的傅里叶系数的性质, 问题 H.6 的开始部分利用了第 II 章的内容; 问题 H.6 的其余部分集中于在 L^2 中的傅里叶变换, 而问题 H.7 探索了在傅里叶变换和卷积之间的重要关联, 它对于第 III 和 IV 章的结果付诸实践.

— 习题 H.1.8(计算 $\int_0^{+\infty} \frac{dt}{1+t^n}$), H.1.9, H.1.10 (欧拉公式 $\sin \pi z = \pi z \prod_{n\geqslant 1}(1 - \frac{z^2}{n^2})$), H.1.11 (互补公式 $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$), H.1.12, H.1.13 (鲁歇定理), H.1.14 和问题 H.9 (解析函数的傅里叶系数, 问题 H.5 和附录 D 的重复回应), H.8 (椭圆函数), H.12 ($\zeta(3)$ 的无理性) 和 H.13 则利用了全纯函数的各种各样的技术. 特别地, 问题 H.8 几乎用遍了第 V 和 VI 章的全部结果.

— 习题 H.1.4, H.1.5, H.1.6 和 H.1.7 给出了计算有理函数或其他函数的傅里叶变换的多种方式 (微分反称的或者留数方法的), 而习题 H.1.6 和 H.1.7 给出了利用泊松公式的例子, 它们对下述问题是个好的练习, 这些问题是: H.10 ($s \mapsto \sum_{n\in\mathbf{Z}} \frac{1}{P(n)^s}$, 其中 P 是个多项式, 这类问题的解析延拓), H.11 (欧拉公式 $q^{1/24}\prod_{n\geqslant 1}(1-q^n) = \sum_{m\in\mathbf{Z}}(-1)^m q^{(6m+1)^2/24}$ 以及其他许多漂亮的公式), 它们被特意设计成能最大地利用第 IV 和 VI 章的陈述.

— 问题 H.14 与课程没有真正的关系: 这是巴黎师范学院的 2003 年的入学考试

的 6 个小时的试题; 它与附录 F 有关.

[554] H.1. 测试题

1. 陈述

1.1. 群的表示

习题 H.1.1. — 设 S_3 是 $\{1,2,3\}$ 的置换群. 以 e, s 和 t 记 S_3 的三个共轭类, 其中 e 是恒同置换的类, s 为对换而 t 为 3-循环.

(i) 证明 (不用构造) S_3 有两个不可约表示, 一个一维, 一个二维.

(ii) 以 χ_1 记平凡表示的特征标, χ_2 记另一个一维表示: 符号差 ε 的特征标为 χ_2, 而 θ 是二维表示 W 的特征标. $\psi = \chi_1 + \chi_2 + 2\theta$ 是什么表示的特征标? 完成下面的表.

	e	s	t
χ_1			
χ_2			
$\chi_1 + \chi_2 + 2\theta$			
θ			

(iii) 将 S_3 以内共轭 (即 $g \cdot x = gxg^{-1}$) 作用于自己, 并以 V 记其相伴的表示而 χ 为其特征标. 计算 χ. 由此推导出 $\mathbf{1}, \varepsilon$ 和 W 在 V 的分解中的重数.

习题 H.1.2. — 试建立 $\{1,2,3,4\}$ 的置换群 S_4 的特征标表. 由于 4 的分拆为 $4, 3+1, 2+2, 2+1+1$ 和 $1+1+1+1$, 故群 S_4 有 5 个共轭类: 中性元 1 的类 C_1 (1 个元), 对换的类 C_2 (6 个元), 具有不交支集的两个对换乘积的类 $C_{2,2}$ (3 个元), 3-循环的类 C_3 (8 个元), 4-循环的类 C_4 (6 个元).

		$\mathbf{1}$	ε	θ	χ_1	χ_2
1	C_1	1	1	2	3	3
6	C_2	1	-1	0	1	-1
3	$C_{2,2}$	1	1	2	-1	-1
8	C_3	1	1	-1	0	0
6	C_4	1	-1	0	-1	1

图 1. S_4 的特征标表

(i) 设 V 是 S_4 在 $\{1,2,3,4\}$ 上作用相伴的置换表示.

[555] (a) 计算 χ_V 和 $\langle \chi_V, \chi_V \rangle$; 由此推导出 V 是两个不同构的不可约表示 V_1 和 V_2 的直和: $V = V_1 \oplus V_2$.

(b) 确定 V 的这两个子空间 V_1 和 V_2, 并返回定义去证明它们是 S_4 的不可约表示.

(c) 计算 V_1 和 V_2 的特征标; 此表中的哪些列是它们填写进去的?

(ii) 第 2 个一维的表示是什么? 我们如何能得到第 2 个 3 维表示 (为什么它是不可约的并且不同于已经构造的那个)?

(iii) 我们如何能完善这个 S_4 的特征标表?

习题 H.1.3. — 设 K 为域, 且 $G \subset \mathbf{GL}_2(K)$ 是形如 $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ 的子群, 其中 $a \in K^*, b \in K$. 让 G 以公式 $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot x = ax + b$ 作用于 K.[1]

(i) 计算 $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1}$. 由此推导出 G 的共轭类为 $C_1 = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$, $N = \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, b \in K - \{0\}\right\}$ 和对于 $a \in K^* - \{1\}$ 的 $D_a = \left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, b \in K\right\}$.

(ii) 从现在开始我们假设 K 为有限域, 基数为 q, 从而 $|G| = q(q-1)$ 以及 $|\mathrm{Conj}(G)| = q$. 以 V 记相伴于 G 在 K 上作用的 G 的置换表示, 而 W 是 V 的一个超平面, 其定义为 $W = \{\sum_{x \in K} \lambda_x e_x, \sum_{x \in K} \lambda_x = 0\}$. 证明 W 是 V 的一个子表示.

(iii) 计算 χ_W; 由此推导出 W 为不可约的.

(iv) G 的其他不可约表示的维数是多少?

(v) 从 K^* 的一个线性特征标出发如何构造 G 的一个特征标? 由此推导出, 如果 $K = \mathbf{F}_5$(其中 $\mathbf{F}_5 = \mathbf{Z}/5\mathbf{Z}$), 则下面是 G 的特征标表:

	$\mathbf{1}$	η	η^2	η^3	χ_W
C_1	1	1	1	1	4
N	1	1	1	1	-1
D_2	1	i	-1	$-i$	0
D_4	1	-1	1	-1	0
D_3	1	$-i$	-1	i	0

图 2. 当 $K = \mathbf{F}_5$ 时, G 的特征标表

[1]我们有 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot x = x$ 和 $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \left(\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \cdot x\right) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot (cx + d) = a(cx+d) + b = acx + (ad + b) = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix} \cdot x$, 而因为 $\begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$, 这证明了我们有一个定义良好的群作用.

(vi) 假设 $q=4$[2]. 请建立 G 的特征标表. 这个表让我们回想起了什么东西? 你能解释这个巧合吗?

1.2. 傅里叶变换和留数方法

习题 H.1.4. — 设 $f:\mathbf{R}\to\mathbf{C}$ 的定义是 $f(t)=\frac{1}{(t+i)^3}$.

[556] (i) 证明 $\hat{f}$ 有定义, 并属于 $\mathscr{C}^1$ 类, 且当 $|t|\to+\infty$ 时有 $|t^N\bar{f}(t)|\to 0$, 其中 $N\in\mathbf{N}$.

(ii) 设 $g:\mathbf{R}\to\mathbf{C}$ 的定义为: 当 $t>0$ 时 $g(t)=e^{-2\pi t}$, 而当 $t\leqslant 0$ 时 $g(t)=0$. 计算 $\hat{g}$; 由此得到 $h(t)=t^2g(t)$ 的傅里叶变换, 然后是 $\hat{f}$.

(iii) 用留数方法重新求出这个结果.(绕一个用心选择的路径对 $F_t(z)=\frac{e^{-2i\pi tz}}{(z+i)^3}$ 积分.)

习题 H.1.5. — (i) 证明, 如果 $a\in\mathbf{C}, f\in L^1(\mathbf{R})$ 而 $\phi\in\mathscr{C}_c^\infty(\mathbf{R})$, 则有 $\int_{\mathbf{R}}\hat{f}(x)(\phi''(x)+a\phi(x))dx=\int_{\mathbf{R}}(a-4\pi^2t^2)f(t)\hat{\phi}(t)dt$. (我们对 $\phi''+a\phi$ 的傅里叶变换感兴趣.)

(ii) 后面我们总假设 $f(x)=\frac{1}{t^2+2i}$. 证明存在 $a\in\mathbf{C}$ 使得有 $\int_{\mathbf{R}}\hat{f}(x)(\phi''(x)+a\phi(x))dx=-4\pi^2\phi(0)$, 其中 $\phi\in\mathscr{C}_c^\infty(\mathbf{R})$.

(iii) 利用留数法证明 $\hat{f}(u)=\frac{\pi}{1+i}e^{-2\pi(1+i)|u|}$.

(iv) 由这个表达式出发重证 (ii).

习题 H.1.6. — 设 $\Omega=\{z\in\mathbf{C},\mathrm{Re}(z)>0\}$.

(i) 设 $\alpha=a+ib\in\Omega$, 又设 $\gamma_R(R>0)$ 是一条闭道, 它由线段 $[0,R],[R,\frac{\alpha R}{a}]$ 和 $[\frac{\alpha R}{a},0]$ 构成. 如果 $n\in\mathbf{N}$, 那么 $\int_{\gamma_R}z^ne^{-z}dz$ 等于什么? 由此得到 $\int_0^{+\infty}t^ne^{-\alpha t}dt=\frac{n!}{\alpha^{n+1}}$.

(ii) 如果 $\lambda\in\mathbf{R}_+^*$, 令 $f_\lambda:\mathbf{R}\to\mathbf{C}$ 是如下定义的函数: 如果 $t\leqslant 0$, 则 $f_\lambda(t)=0$, 而如果 $t\geqslant 0$, 则 $f_\lambda(t)=te^{-\lambda t}$. 计算 $\hat{f}_\lambda(x)$, 其中 $x\in\mathbf{R}$.

(iii) 我们留意到 $x\mapsto x\hat{f}_\lambda(x)$ 不是可和的. 在没有计算 $\hat{f}_\lambda$ 的情形下能知道这一点吗? (区别 $\hat{f}_\lambda$ 不可和与 $\hat{f}_\lambda$ 可和.)

(iv) 对于任意的 $\lambda\in\mathbf{R}_+^*$, 建立公式 $\sum_{n\in\mathbf{Z}}\frac{1}{(\lambda+2i\pi n)^2}=\frac{e^\lambda}{(e^\lambda-1)^2}$.

(v) 然后得到对 $\sum_{n\in\mathbf{Z}}\frac{(-1)^n}{(\lambda+2i\pi n)^2}$ 的类似公式?

(vi) 证明 $\sum_{n\in\mathbf{Z}}\frac{1}{(z+2i\pi n)^2}$ 对于所有 $z\notin 2i\pi\mathbf{Z}$ 均收敛, 而其和等于 $\frac{e^z}{(e^z-1)^2}$.

习题 H.1.7. — 如果 $z\in\mathbf{C}$, 定义 $\cosh z=\frac{e^z+e^{-z}}{2},\sinh z=\frac{e^z-e^{-z}}{2}$. 我们要用到一个囿于下的不等式 $|\cosh(x+iy)|\geqslant\frac{e^{|x|}-e^{-|x|}}{2}$.

(i) 证明 $z\mapsto\cosh\pi z$ 全纯. 它的导数是什么? 零点是哪些?

(ii) 如果 $u\in\mathbf{R}$, 以 f_u 记函数 $z\mapsto e^{-2i\pi uz}\frac{1}{\cosh\pi z}$. 计算 $I(R)=\int_{\gamma_R}f_u(z)dz$, 其中 γ_R 为由线段 $[-R,R],[R,R+i],[R+i,-R+i]$ 和 $[-R+i,-R]$ 组成的闭道.

(iii) 推导: 如果 $y>0$, 则 $t\mapsto g_y(t)=\frac{1}{\cosh\pi yt}$ 的傅里叶变换是 $x\mapsto\frac{1}{y}\frac{1}{\cosh(\pi x/y)}$. (先

[2] 于是有 $K=\mathbf{F}_2[X]/(X^2+X+1)$, 但回答此问题不一定需要知道是如何构造 K 的.

考虑 $y=1$ 的情形.)

(iv) 如果 $a \in \mathbf{R}$, 以 Ω_a 记半平面 $\mathrm{Re}(z)>a$. 证明级数 $\sum_{n\in\mathbf{Z}} \frac{1}{\cosh n\pi z}$ 对所有的 $z \in \Omega_0$ 收敛, 记其和为 $F(z)$. 证明如此定义的函数 $z \mapsto F(z)$ 满足函数方程 $F(\frac{1}{z}) = zF(z)$, $z \in \Omega_0$.(先处理 z 为实的情形.)

习题 H.1.8. — 设 $n \geqslant 2$ 为整数, 且 $\theta \in [0,\pi]$ 不是形如 $\frac{(2k+1)\pi}{n}(k \in \mathbf{N})$ 的数. 如果 $R>1$, 令 $I_1(R), I_2(R)$ 和 $I_3(R)$ 分别是 $\frac{dz}{1+z^n}$ 在线段 $[0,R]$, 以 0 为圆心的从 R 到 $e^{i\theta}R$ 的圆弧以及线段 $[e^{i\theta}R, 0]$ 上的积分. (请画出来.)

(i) 计算 $I_1(R)+I_2(R)+I_3(R)$.

(ii) $I_1(R), I_2(R)$ 和 $I_3(R)$ 当 $R \to +\infty$ 时的极限是什么?

(iii) 明智地选择 θ 以得出 $\int_0^{+\infty} \frac{dt}{1+t^n}$ 的值.

1.3. 全纯函数 [557]

习题 H.1.9. — (i) 证明 $\tan = \frac{\sin}{\cos}$ 是它在 0 的泰勒级数在 $]\frac{-\pi}{2}, \frac{\pi}{2}[$ 上的和.

(ii) $\frac{\sin \pi z}{z-1}$ 在 0 的泰勒级数的收敛半径是什么?

习题 H.1.10. — 如果 $z \in \mathbf{C}$, 令 $\sin z = \frac{e^{iz}-e^{-iz}}{2i}$. 当 $z=(k+\frac{1}{2})\pi + iy(k \in \mathbf{Z})$ 或者 $z = x+iy(|y| \geqslant \frac{\pi}{2})$ 时我们有 $|\sin z| \geqslant 1$(在后面的情形有 $|\sin z| \geqslant \frac{1}{2}(e^{\pi/2} - e^{-\pi/2})$).

(i) 证明乘积 $\prod_{n\geqslant 1}(1-\frac{z^2}{n^2})$ 对所有的 $z \in \mathbf{C}$ 收敛, 而如此定义的函数 $z \mapsto F(z)$ 在 $\mathbf{C}$ 上全纯.

(ii) 证明 $G(z) = \frac{\pi z}{\sin \pi z}F(z)$ 在 $\mathbf{C}$ 上为偶的全纯函数并不取零值.

(iii) 由此得到, 存在一个 $\mathbf{C}$ 中的序列 $(a_n)_{n\geqslant 1}$ 使得

- 对每个 $z \in \mathbf{C}$, 级数 $\sum_{n\geqslant 1} a_n z^n$ 收敛,
- 如此定义的函数 $z \mapsto g(z)$ 对所有 $z \in \mathbf{C}$ 满足 $e^{g(z)} = G(z)$.

(iv) 如果 N 是一个 $\geqslant 1$ 的整数, 以 C_N 记 $|G(z)|$ 在顶点为 $\pm(N+\frac{1}{2}) \pm i(N+\frac{1}{2})$ 的正方形 (即 $\{x+iy, -(N+\frac{1}{2}) \leqslant x, y \leqslant N+\frac{1}{2}\}$) 上的最大值, 又令 $R_N = \sqrt{2}(N+\frac{1}{2})$. 证明 $C_N \leqslant \pi R_N (R_N^2+1)^N e^{\sum_{n\geqslant N+1} R_N^2/n^2}$. 由此得到, 当 $k \geqslant 2$ 时有 $N^{-k}\log C_N \to 0$.

(v) 因此得到当 $n \geqslant 2$ 时 $a_n = 0$.(将 a_n 写成形如 $|a_n|e^{i\alpha_n}$, 其中 $\alpha_n \in [0, 2\pi[$, 再计算 $I_n(r) = \int_0^{2\pi}(1+\cos(n\theta+\alpha_n))\mathrm{Re}(g(re^{i\theta}))d\theta$, 并求 $I_n(r)$ 的囿于上的优函数.)

(vi) 证明对所有的 $z \in \mathbf{C}$ 有 $F(z) = \frac{\sin \pi z}{\pi z}$.

习题 H.1.11. — 回顾: Γ 函数是 $\mathbf{C}$ 上的一个亚纯函数, 它除了在 $-n(n \in \mathbf{N})$ 的单极点外全纯, 并在整个带形 $0<a \leqslant \mathrm{Re}(s) \leqslant b$ 上满足函数方程 $\Gamma(s+1) = s\Gamma(s), s \notin -\mathbf{N}$, 又 $\Gamma(1)=1$.

(i) 证明 $s \mapsto F(s) = \sin \pi s \Gamma(s)\Gamma(1-s)$ 在 $\mathbf{C}$ 上全纯, 是个周期为 1 的周期函数.

(ii) 由此推出, 存在在 $\mathbf{C}^*$ 上的全纯函数 f 使得对所有的 $s \in \mathbf{C}$ 有 $F(s) = f(e^{2i\pi s})$.

(iii) 证明存在 $a_n \in \mathbf{C}, n \in \mathbf{N}$ 使得对所有的 $z \in \mathbf{C}^*$ 有 $f(z) = \sum_{n\in\mathbf{Z}} a_n z^n$, 并且对所有的 $T \in \mathbf{R}$ 有 $a_n = \int_{[iT,1+iT]} e^{-2i\pi s} F(s) ds$.

(iv) 证明 $s \mapsto e^{-\pi|\mathrm{Im}(s)|} F(s)$ 在 $\mathbf{C}$ 上有界.(可引入形如 $1 \leqslant \mathrm{Re}(s) \leqslant 2$ 和 $|\mathrm{Im}(s)| \geqslant 1$ 的集合.)

(v) 由此推出互补公式: 对于所有的 $s \notin \mathbf{Z}$, $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$.

习题 H.1.12. — 如果 g 是 $\mathbf{C}$ 上的亚纯函数, 且 $N \in \mathbf{N}$; $g = O(y^N)$ 是说, 存在 $C, M \in \mathbf{R}$ 使得当 $|y| \geqslant M$ 时有 $|g(x+iy)| \leqslant C|y|^N$.

(i) 证明如果 g 是 $O(y^N)$ 的, 则 g' 是 $O(y^{N-1})$ 的.

(ii) 设 f 是 $\mathbf{C}$ 上的一个亚纯的周期为 1 的周期奇函数, 同时在留数为 1 的整数单极点之外全纯, 并是 $O(y^N)$ 的. 证明 $f^2 + f'$ 为常数.

习题 H.1.13. — 设 $D = D(0,1)$ 而 $C = \partial D$ 为半径为 1 中心在 0 的圆. 又设 Ω 是包含 D 的一个开集而 f 是 Ω 上的全纯函数并在 C 上不取零, 设 g 是在 Ω 上的另一个全纯函数使得当 $z \in C$ 时有 $|f(z) - g(z)| < |f(z)|$.

(i) 证明存在包含 C 的开集 $\Omega' \subset \Omega$ 以及在 Ω' 上的全纯函数 h 使得在 Ω' 上有 $\frac{g}{f} = e^h$. h' 是什么?

(ii) 证明 f 和 g 在 D 中有相同的零点数 (计入重数).

(iii) 设 G 在 Ω 上全纯使得当 $z \in C$ 时有 $|G(z)| < 1$. 证明 $G(D) \subset D$ 且 G 在 D 中只有唯一一个不动点.

[558] **习题 H.1.14.** — (i) 设 $x \in \mathbf{R}_+^*$. 证明级数 $\sum_{n\in\mathbf{N}} \frac{1}{(n+x)^s}$ 在 $\mathrm{Re}(s) > 1$ 上收敛, 且这个级数的和 $F(x,s)$ 在半平面 $\mathrm{Re}(s) > 1$ 上对 s 全纯.

(ii) 建立公式: 如果 $\mathrm{Re}(s) > 1$, 则 $F(x,s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} \frac{e^{-tx}}{1-e^{-t}} t^{s-1} dt$.

(iii) 证明 $F(x,s)$ 具有到 $\mathbf{C}$ 的亚纯延拓, 它在 $s=1$ 是留数为 1 的单极点, 在除了此单极点外全纯.

2. 习题校正

习题 H.1.1. (i) 由于 S_3 具有三个等价类, 故它也具有三个不可约表示 W_1, W_2 和 W_3, 并根据 Burnside 公式 $(\dim W_1)^2 + (\dim W_2)^2 + (\dim W_3)^2 = 6$, 知其仅有的可能性是两个维数为 1 而第三个的维数为 2.

(ii) 按照推论 I.2.23 的 (i), $\psi = \chi_1 + \chi_2 + 2\theta$ 是正则表示的特征标; 因此根据对正则表示特征标的一般公式 (I.1 的 2.3 小节) 有 $\psi(e) = 6, \psi(s) = 0$ 和 $\psi(t) = 0$. 这给出了以下表格:

(iii) 由于 V 是一个置换表示, 于是 $\chi(g)$ 是 g 的不动点的个数 (I.1 的 2.3 小节), 就是说, S_3 的使得 $ghg^{-1} = h$ 的元 h 的个数, 或者说是与 g 交换的元的个数, 因此有 $\chi(g) = |Z_g| = |S_3| \cdot |C_g|^{-1}$. 由此得到 $\chi(e) = 6, \chi(s) = 2$ 和 $\chi(t) = 3$.

	e	s	t
χ_1	1	1	1
χ_2	1	-1	1
$\chi_1+\chi_2+2\theta$	6	0	0
θ	2	0	-1

根据推论 I.2.18, W' 在 V 中的重数是 $\langle\chi_{W'},\chi\rangle$. 因为

$$\langle\chi_1,\chi\rangle=\frac{1}{6}(6+3\cdot(1\cdot 2)+2\cdot(1\cdot 3))=3,$$
$$\langle\chi_2,\chi\rangle=\frac{1}{6}(6+3\cdot(-1\cdot 2)+2\cdot(1\cdot 3))=1,$$
$$\langle\theta,\chi\rangle=\frac{1}{6}(2\cdot 6+3\cdot(0\cdot 2)+2\cdot(-1\cdot 3))=1,$$

故 $V=3\cdot\mathbf{1}\oplus\varepsilon\oplus W$.

习题 H.1.2. (i) (a) 由于 V 是置换表示, $\chi_V(\sigma)$ 是 σ 作用在 $\{1,2,3,4\}$ 上的不动点的个数 (I.1 的 2.3 小节). 因此有 $\chi_V(C_1)=4,\chi_V(C_2)=2,\chi_V(C_{2,2})=0,\chi_V(C_3)=1$ 而 $\chi_V(C_4)=0$.

标量积 $\langle\chi_V,\chi_V\rangle$ 等于 $\frac{1}{24}(4^2+6\cdot 2^2+3\cdot 0^2+8\cdot 1^2+6\cdot 0^2)=2$. 如果 $V=\oplus_{W\in\mathrm{Irr}(S_4)}m_W W$, 因为这些 χ_W 是个法正交族 (定理 I.2.14), 故这个标量积也等于 $\sum_{W\in\mathrm{Irr}(S_4)}m_W^2$, 而由于 2 的唯一的表示成两个平方数之和的是 1^2+1^2, 因此得到正好与两个 $W\in\mathrm{Irr}(S_4)$ 使得 $m_V=1$, 其余的 $m_V=0$. 断言得证.

(b) 由 $e_1+\cdots+e_4$ 生成的直线 V_1 和方程为 $x_1+\cdots+x_4$ 的超平面 V_2 在 S_4 下稳定. 因为 V_1 的维数为 1, 故自动为不可约的.

设 $x=(x_1,x_2,x_3,x_4)\in V_2$ 非零. 要证明的是, V_2 的由 $\sigma\cdot x(\sigma\in S_4)$ 生成的子空间 U_x 等于 V_2. 存在 $i\neq j$ 使得 $x_i\neq x_j$. 设 τ 为对换 (ij). 于是 $x-\tau\cdot x$ 是 e_i-e_j 的一个非零倍数, 由此可知 e_i-e_j 属于 U_x, 故对所有 $\sigma\in S_4$, $\sigma\cdot(e_i-e_j)=e_{\sigma(i)}-e_{\sigma(j)}$ 也属于它. 由于 $(\sigma(i),\sigma(j))$ 当 σ 遍历 S_4 时遍历了 $\{1,2,3,4\}$ 的所有不同元的偶对, [559] 这便证明了 U_x 包含了 e_1-e_2,e_1-e_3 和 e_1-e_4, 而由于这三个向量生成了 V_2, 从而得到了结论.

(c) 表示 V_1 是个平凡的表示, 从而对于所有的 $C\in\mathrm{Conj}(S_4)$ 有 $\chi_{V_1}(C)=1$. 由于 $\chi_{V_1}+\chi_{V_2}=\chi_V$, 这让我们可以决定出 χ_{V_2} 并填进表格中的第一和第四列.

(ii) (a) 第二个 1 维表示是符号差 ε; 它的值已在第二列显示出来. 第二个 3 维表示是 $V_1\otimes\varepsilon$; 如果它可分解为 $V_1\otimes\varepsilon=W_1\oplus W_2$ 的形式, 那么 $V_1=(V_1\otimes\varepsilon)\otimes\varepsilon$ 可以分解为形如 $(W_1\otimes\varepsilon)\oplus(W_2\otimes\varepsilon)$, 这是荒谬的. 我们有 $\chi_{V_1\otimes\varepsilon}(g)=\chi_{V_1}(g)\varepsilon(g)$ (I.1 的 2.1 小节), 因此 $\chi_{V_1\otimes\varepsilon}(C_2)=-1$ 不同于 $\chi_{V_1}(C_2)=1$, 这证明 $V_1\otimes\varepsilon$ 与 V_1 的特征标不同, 从而不同构.

(b) 由于 S_4 有 5 个共轭类, 从而有 5 个不可约表示 (推论 I.2.16). 如果以 d 记那个缺少的表示且 θ 是它的特征标, 那么 Burnside 公式表明 $24 = 1^2 + 1^2 + 3^2 + 3^2 + d^2$, 从而 $d = 2$. 为了填写最后一列, 我们利用 $1 + \varepsilon + 2\theta + 3\chi_1 + 3\chi_2$ 是正则表示的特征标这个事实 (推论 I.2.23 的 (i)), 而它是已知的 (I.1 的 2.3 小节).

习题 H.1.3. (i) 我们有 $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} c & ad + (1-c)b \\ 0 & 1 \end{pmatrix}$. 由此得到 $\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ 的共轭是形如 $\begin{pmatrix} c & d' \\ 0 & 1 \end{pmatrix}$ 的元, 如果 $c \neq 1$, 那么所有这种形式的元都是 $\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$ 的一个共轭. 这些 $D_a(a \in K^* - \{1\})$ 因而组成了这些共轭类. 另外, C_1 是中性元的共轭类, 而因为当 $a \neq 0$ 时有 $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, 故 N 是 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 的共轭类.

(iii) 我们有 $g \cdot (\sum_{x \in K} \lambda_x e_x) = \sum_{x \in K} \lambda_x e_{g \cdot x} = \sum_{x \in K} \lambda_{g^{-1} \cdot x} e_x$. 但是 $x \mapsto g^{-1} \cdot x$ 是 K 的一个双射, 从而 $\sum_{x \in K} \lambda_{g^{-1} \cdot x} = \sum_{x \in K} \lambda_x$, 这便证明了, 当 $v = \sum_{x \in K} \lambda_x e_x \in W$ 时有 $g \cdot v = \sum_{x \in K} \lambda_{g^{-1} \cdot x} e_x \in W$.

(iv) V 是个置换表示, 从而 $\chi_V(g)$ 是 g 作用在 K 上的不动点的个数. 因此要计算方程 $ax + b = x$ 在 K 中的解的个数, 这给出了 $\chi_V(C_1) = q, \chi_V(N) = 0$, 而当 $a \in K^* - \{1\}$ 时有 $\chi_V(D_a) = 1$.

现在 V 是 W 和由 $\sum_{x \in K} e_x$ 生成的直线的直和, 而 G 在此直线上的作用为平凡的. 于是得到 $\chi_V(g) = \chi_W(g) + 1$, 我们便由此有 $\chi_W(C_1) = q - 1, \chi_W(N) = -1$ 和 $\chi_W(D_a) = 0$, 其中 $a \in K^* - \{1\}$.

于是 $\langle \chi_W, \chi_W \rangle = \frac{1}{q(q-1)}((q-1)^2 + |N| \cdot 1^2 + \sum_{a \in K^* - \{1\}} |D_a| \cdot 0^2) = \frac{1}{q(q-1)}((q-1)^2 + (q-1)) = 1$, 由此并用推论 I.2.21 便得到了 W 的不可约性.

(v) 由于按照推论 I.2.16 有 $|\mathrm{Irr}(G)| = |\mathrm{Conj}(G)|$, 又由于 $|\mathrm{Conj}(G)| = q$, 故有另外的 $q-1$ 个不可约表示. 以 $d_1, \ldots, d_{q-1}$ 记它们的维数. Burnside 公式给出了 $q(q-1) = |G| = (\dim W)^2 + \sum_{i=1}^{q-1} d_i^2$, 但 $\dim W = q - 1$, 故有 $\sum_{i=1}^{q-1} d_i^2 = q(q-1) - (q-1)^2 = q - 1$. $q-1$ 个 $\geqslant 1$ 的整数的平方和等于 $q-1$ 只能是所有的整数全为 1, 由此可知其他的 $q-1$ 个 G 的表示的维数必为 1 (即均为线性特征标).

(vi) 如果 χ 是 K^* 的一个线性特征标, 则 $\chi \circ \det$ 是 G 的一个线性特征标. 群 $\mathbf{F}_5^*$ 是由 2 生成的 4 阶循环群 (我们有 $2^2 = 4, 2^3 = 8 = 3, 2^4 = 16 = 1$). $\mathbf{F}_5^*$ 的特征标因而被它在 2 的值决定, 应该是 4 次单位根 (即 $1, i, -1, -i$). 故而有 4 个这样的特征标, 如果以 η 记 $\eta(2) = i$ 的特征标, 其余的便是 η^2, η^3 和 η^4, 后者就是平凡特征标. 我们要找的这 4 个 G 的特征标因而恰好是 $\eta^i \circ \det, 0 \leqslant i \leqslant 3$, 它给出了所说的表.

(vii) 群 K^* 的基数为 3 从而为循环群, 由任意的 $a \neq 1$ 生成. (如果 K 为有限域, 则 K^* 总是循环群; 在这里的情形, 如果 $a \in K^* - \{1\}$, 则由 a 生成的子群的基数整除 $|K^*| = 3$, 因此等于 3, 表明这个子群就是 K^*.) K^* 的线性特征标从而由它在 a 的值决定, 它是三次单位根. 有 3 个这样的特征标, 如果 η 为 $\eta(a) = j = e^{2i\pi/3}$, 其余的便是 η^2 和 $\eta^3 = \mathbf{1}$. 它们给出的表如下 (图 3). [560]

	$\mathbf{1}$	η	η^2	χ_W
C_1	1	1	1	3
N	1	1	1	-1
D_a	1	j	j^2	0
D_{a^2}	1	j^2	j	0

图 3. 当 $K = \mathbf{F}_4$ 时 G 的特征标表

我们认出它是 A_4 的特征标表, 这没有什么奇怪的, 因为 G 同构于 A_4. 实际上, 选取 K 与 $\{1,2,3,4\}$ 之间的一个双射便将 G 在 K 上的作用转变为 G 在 $\{1,2,3,4\}$ 上的作用, 从而给出了 G 到 S_4 的一个单射. 这个单射的像 H 因而是一个同构于 G 的 S_4 的子群. 一个这样的群在 S_4 中为正规的: 如果 $g \notin H$, 由于基数的原因, 便有 $gH = Hg = S_4 - H$(注意, $|H| = |G| = 12 = |A_4|$, 而 $|S_4| = 24 = 2|H|$), 故 $gHg^{-1} = Hgg^{-1} = H$. 商群 G/H 的级数等于 2, 从而同构于 $\{\pm 1\}$, 它给出了一个线性特征标 $\eta : S_4 \to \{\pm 1\}$. η 在 A_4 上的限制仍是一个线性特征标, 但 A_4 的特征标取值于 $\boldsymbol{\mu}_3$, 这表明在 A_4 上 $\eta = 1$; 换句话说, A_4 包含在 η 的核 H 中, 由于基数的关系它们相等. 由此有 $G \cong A_4$. (我们也可注意到, D_a 或 D_{a^2} 的一个元的像是一个 3-循环, 因而出现在 A_4 中, 而因为 $D_a \cup D_{a^2}$ 的基数 $8 > \frac{|G|}{2}$, 故 G 由 $D_a \cup D_{a^2}$ 生成, 从而不包含在 G 的一个真子群中, 再利用 K 为特征 2 的域, 我们也可以直接证明 N 的一个元的像是两个对换的乘积, 从而属于 A_4.)

习题 H.1.4. (i) 函数 f 与 $t \mapsto tf(t)$ 同样可和, 由此得到 (由定理 IV.2.8 的 (ii)) $\hat{f}$ 确有定义并属于 $\mathscr{C}^1$. 另外, f 属于 $\mathscr{C}^\infty$, 而 $f^{(N)}(t) = \frac{(-3)(-4)\cdots(-N-2)}{(t+i)^{3+N}}$ 是可和的; 由此知 (由定理 IV.2.8 的 (i)), 当 $|t| \to +\infty$ 时 $|t^N \hat{f}(t)| \to 0$, 其中 $N \in \mathbf{N}$.

(ii) $\hat{g}(x) = \int_0^{+\infty} e^{-2\pi t(1+ix)} dt = [\frac{e^{-2\pi t(1+ix)}}{-2\pi(1+ix)}]_0^{+\infty} = \frac{1}{2\pi(1+ix)}$. 由于 $t^2 g(t)$ 可和, 它的傅里叶变换是 $\frac{1}{(-2i\pi)^2}\hat{g}^{(2)}(x) = \frac{2}{(2i\pi)^3}\frac{1}{(x-i)^3}$ (定理 IV.2.8 的 (ii)); 特别地, 它可和, 并可应用在 L^1 中的傅里叶反演公式, 从而给出了 $\overline{\mathscr{F}}(\frac{2}{(2i\pi)^3}\frac{1}{(x-i)^3}) = t^2 g(t)$. 由于 $\overline{\mathscr{F}}(\frac{1}{(x-i)^3})(t) = \int_{\mathbf{R}} e^{2i\pi tx}\frac{1}{(x-i)^3}dx = (-1)^3 \hat{f}(t)$, 借助于变量变换 $x = -y$, 最后我们得到 $\hat{f}(t) = \frac{(-2i\pi)^3}{2}t^2 g(t)$.

(iii) 函数 $F_t(z)$ 在 $\mathbf{C}$ 上亚纯, 并在 $z = -i$ 的 3 阶极点之外全纯, 且因为

$$e^{-2i\pi tz} = e^{-2\pi t}e^{-2i\pi t(z+i)} = e^{-2\pi t}(1 - 2i\pi t(z+i) + \frac{1}{2}(2i\pi t(z+i))^2 + \cdots),$$

于是有 $F_t(z)=e^{-2\pi t}(\frac{1}{(z+i)^3}-\frac{2i\pi t}{(z+i)^2}+\frac{(2i\pi t)^2}{2(z+i)}+\cdots)$, 从而 $\mathrm{Res}(F_t,-i)=\frac{(2i\pi)^2}{2}t^2e^{-2\pi t}$.

[561] 设 $t\geqslant 0$. 如果 $R>1$, 令 γ_R 为线段 $[-R,R]$ 和半圆 C_R^- 构成的半圆弧, 其参数表示为 $t\mapsto Re^{-i\pi t}, t\in[0,1]$. 令

$$I_1(R)=\int_{[-R,R]}F_t(z)dz \quad 和 \quad I_2(R)=\int_{C_R^-}F_t(z)dz.$$

我们有指标 $I(\gamma_R,-i)=-1$, 故

$$I_1(R)+I_2(R)=\int_{\gamma_R}F_t(z)dz=2i\pi I(\gamma_R,-i)\mathrm{Res}(F_t,-i)=\frac{(-2i\pi)^3}{2}t^2e^{-2\pi t},$$

其中 $R>1$. 但当 $R\to+\infty$ 时 $I_1(R)\to\hat{f}(t)$. 另外, 如果 $\mathrm{Im}(z)\leqslant 0$, 则 $|e^{-2i\pi tz}|\leqslant 1$, 而如果 $z\in C_R^-$, 则 $|z+i|\geqslant|z|-1=R-1$; 由此知, 当 $z\in C_R^-$ 时有囿于上的不等式 $|F_t(z)|\leqslant\frac{1}{(R-1)^3}$. 因此当 $R\to+\infty$ 时 $|I_2(R)|\leqslant\frac{1}{(R-1)^3}\lg(C_R^-)=\frac{\pi R}{(R-1)^3}\to 0$. 取极限给出了 $\hat{f}(t)=\frac{(-2i\pi)^3}{2}t^2e^{-2\pi t}$.

如果 $t\leqslant 0$, 则将半圆周 C_R^- 换作在上半平面的半圆周 C_R^+. 我们有 $I(\gamma_R,-i)=0$, 以与上面相同的方法可证明 $\hat{f}(t)=0$.

习题 H.1.5. (i) 如果 ϕ 属于 $\mathscr{C}^\infty$ 且具有紧支集, 那么它的导数也如此, 于是由定理 IV.2.5 的 (i) 得到 $\phi^{(n)}$ 的傅里叶变换为 $t\mapsto(2i\pi t)^n\hat{\phi}(t)$; 因此 $\phi''+a\phi$ 的傅里叶变换是 $t\mapsto(a-4\pi^2t^2)\hat{\phi}(t)$, 那么我们要求的公式是命题 IV.3.24 的公式, 即它是对所有 $f,g\in L^1(\mathbf{R})$ 都成立的 $\int_{\mathbf{R}}\hat{f}(x)g(x)dx=\int_{\mathbf{R}}f(t)\hat{g}(t)dt$ 的一个特殊情形.

(ii) 在 $f(t)=\frac{1}{t^2+2i}$ 以及 $a=-8i\pi^2$ 的情形, 根据 (i), 我们得到 $\int_{\mathbf{R}}\hat{f}(x)(\phi''(x)+a\phi(x))=-4\pi^2\int_{\mathbf{R}}\hat{\phi}(t)dt$. 但根据在 $\mathscr{S}(\mathbf{R})$ 中的反演公式 (定理 IV.3.14) 我们知道 $\int_{\mathbf{R}}\hat{\phi}(t)dt$ 是 $\hat{\phi}$ 的傅里叶反演在 0 的值, 即 $\phi(0)$.

(iii) 为了计算 f 的傅里叶变换 $u\mapsto\hat{f}(u)$, 引进函数 g_u, 其定义是 $g_u(z)=e^{-2i\pi uz}\frac{1}{z^2+2i}$, 它在 $\mathbf{C}$ 上亚纯, 而除了在 $1-i$ 和 $i-1$ 的单极点外全纯, 并且 $\mathrm{Res}(g_u,1-i)=e^{-2i\pi u(1-i)}\frac{1}{2(1-i)}=\frac{1}{2-2i}e^{-2\pi u(1+i)}$ 及 $\mathrm{Res}(g_u,i-1)=\frac{1}{2i-2}e^{2\pi u(1+i)}$.

如果 $u\geqslant 0$, 我们对 $g_u(z)dz$ 在由线段 $[-R,R]$ 和中心在 0 半径为 R 的下半圆周组成的闭道上积分. 如果 $R>\sqrt{2}$, 我们有 $I(\gamma_R,1-i)=-1$ 和 $I(\gamma_R,i-1)=0$, 那么留数公式给出了

$$\int_{\gamma_R}g_u(z)dz=-2i\pi\mathrm{Res}(g_u,1-i)=\frac{\pi}{1+i}e^{-2\pi u(1+i)}.$$

现在, 当 $R\to+\infty$ 时, 在 $[-R,R]$ 上的此积分趋向 $\hat{f}(u)$, 而在半圆周上具有囿于上的不等式 $|e^{-2i\pi uz}|\leqslant 1$ 和 $|\frac{1}{z^2+2i}|\leqslant\frac{1}{R^2-2}$. 由于半圆周的长为 πR, 故在此半圆上的这个积分的模被 $\frac{\pi R}{R^2-2}$ 囿于上, 从而当 $R\to+\infty$ 时趋向 0. 取极限便给出了 $\hat{f}(u)=\frac{\pi}{1+i}e^{-2\pi u(1+i)}$.

如果 $u<0$, 我们在由线段 $[-R,R]$ 和中心在 0 半径为 R 的上半圆周构成的道路 γ_R^+ 上积分. 如果 $R>\sqrt{2}$, 则有 $I(\gamma_R,1-i)=0$ 和 $I(\gamma_R,i-1)=1$, 而与上面同样的推理给出了 $\hat{f}(u)=\frac{\pi}{1+i}e^{2\pi u(1+i)}$. (我们也可利用 f 的奇偶性得到 $\hat{f}$ 的傅里叶变换.)

(iv) 分部积分给出了[3]

$$\int_0^{+\infty}e^{-2\pi(1+i)u}\phi''(u)du=[\phi'(u)e^{-2\pi(1+i)u}]_0^{+\infty}+2\pi(1+i)\int_0^{+\infty}e^{-2\pi(1+i)u}\phi'(u)du$$
$$=-\phi'(0)-2\pi(1+i)\phi(0)+(2\pi(1+i))^2\int_0^{+\infty}e^{-2\pi(1+i)u}\phi(u)du,$$

同样地, [562]

$$\int_{-\infty}^0 e^{2\pi(1+i)u}\phi''(u)du=\phi'(0)-2\pi(1+i)\phi(0)+(2\pi(1+i))^2\int_{-\infty}^0 e^{2\pi(1+i)u}\phi(u)du,$$

从而

$$\int_{\mathbf{R}}\hat{f}(u)(\phi''(u)-8i\pi^2\phi(u))du=\frac{\pi}{1+i}(-4\pi(1+i)\phi(0))=-4\pi^2\phi(0).$$

即为所求.

习题 H.1.6. 函数 e^{-z} 在 $\mathbf{C}$ 上全纯, 而 $\mathbf{C}$ 可缩. 因此它在所有闭道上的积分为 0(注记 VI.1.4 或留数公式). 由此得到

$$\int_0^R t^ne^{-t}dt+\int_0^{\frac{bR}{a}}(R+it)^ne^{-R-it}idt+\int_R^0(\alpha t)^ne^{-\alpha t}\alpha dt=0.$$

当 $R\to+\infty$ 时, 则有 $\int_0^R t^ne^{-t}dt\to\int_0^{+\infty}t^ne^{-t}dt=n!$ 和

$$|\int_0^{\frac{bR}{a}}(R+it)^ne^{-R-it}idt|\leqslant e^{-R}\int_0^{\frac{bR}{a}}|(R+it)|^ndt$$
$$\leqslant e^{-R}\frac{bR}{a}(R^2+(\frac{bR}{a})^2)^{n/2}\to 0.$$

由于 $\int_R^0(\alpha t)^ne^{-\alpha t}\alpha dt\to-\alpha^{n+1}\int_0^{+\infty}t^ne^{-\alpha t}dt$, 则取极限得到了 $\alpha^{n+1}\int_0^{+\infty}t^ne^{-\alpha t}dt=n!$. 得到结论.

(ii) 因为 $\lambda+2i\pi x\in\Omega$, 那么根据 (i) 有

$$\hat{f}_\lambda(x)=\int_{\mathbf{R}}e^{-2i\pi xt}f_\lambda(t)dt=\int_0^{+\infty}te^{-(\lambda+2i\pi x)t}dt=\frac{1}{(\lambda+2i\pi x)^2}.$$

(iii) 如果 $\hat{f}_\lambda$ 不是可和的, 于是因由黎曼 – 勒贝格定理知 $\hat{f}_\lambda$ 是连续的, 故它在 $[-1,1]$ 上可和, 从而在 $\mathbf{R}-[-1,1]$ 不可和. 由于在 $\mathbf{R}-[-1,1]$ 上 $|x\hat{f}_\lambda(x)|\geqslant|\hat{f}_\lambda(x)|$, 这表明 $x\hat{f}_\lambda(x)$ 既不在这个开集上可和更不在 $\mathbf{R}$ 上可和.

[3] 这个计算可以重新解释为, 在分布函数 (或广义函数) 的意义下, $\hat{f}$ 是微分方程 $u''-8i\pi^2u=-4\pi^2\delta_0$ 的解, 其中 δ_0 是狄拉克 (Dirac) 分布函数在 0 的质量.

如果 $\hat{f}_\lambda$ 可和且 $x\hat{f}_\lambda(x)$ 也可和, 则根据定理 IV.2.8 的 (ii) 知 $\mathscr{F}\hat{f}_\lambda$ 属于 $\mathscr{C}^1$ 类, 且 $\mathscr{F}(x\hat{f}_\lambda(x))(t) = \frac{-1}{2i\pi}(\mathscr{F}\hat{f}_\lambda)'(t)$. 现在, 将在 L^1 中的傅里叶反演公式用于 f_λ 便证明了 $(\mathscr{F}\hat{f}_\lambda)(t) = f_\lambda(-t)$. 因为 f_λ 在 0 不可微, 故我们得到了一个矛盾; 由此表明 $x\hat{f}_\lambda(x)$ 不可和.

(iv) 函数 $\hat{f}_\lambda$ 及其导数在无限远是 $O(|x|^{-2})$ 的. 因此可以将泊松公式用于它. 除此之外, $\hat{f}_\lambda$ 可和, 于是在 L^1 中的傅里叶反演公式可用于 f_λ, 从而证明了 $(\mathscr{F}\hat{f}_\lambda)(t) = f_\lambda(-t)$. 因此泊松公式变成了

$$\sum_{n\in\mathbf{Z}} \frac{1}{(\lambda+2i\pi n)^2} = \sum_{n\in\mathbf{Z}} \hat{f}_\lambda(n) = \sum_{n\in\mathbf{Z}} f_\lambda(-n) = \sum_{n=0}^{+\infty} ne^{-n\lambda}$$
$$= -(\sum_{n=0}^{+\infty} e^{-n\lambda})' = -(\frac{1}{1-e^{-\lambda}})' = \frac{e^{-\lambda}}{(1-e^{-\lambda})^2} = \frac{e^{\lambda}}{(e^{\lambda}-1)^2}.$$

(求导与求级数交换的合理性在于我们涉及的是 ($e^{-\lambda}$ 的) 整级数.)

(v) 注意 $(-1)^n = e^{i\pi n}$. 于是对其傅里叶变换是 $t \mapsto f_\lambda(\frac{1}{2}-t)$ 的 $e^{i\pi x}\hat{f}_\lambda(x)$ 用泊松公式来求值.

(vi) 如果 K 是 $\mathbf{C} - 2i\pi\mathbf{Z}$ 的一个紧集, 则存在 $R > 0$ 使得对所有的 $z \in K$ 有 $|z| \leqslant R$. 如果 $|n| > \frac{R}{2\pi}$, 则有 $|\frac{1}{(z+2i\pi n)^2}| \leqslant \frac{1}{(2\pi|n|-R)^2}$, 并由于 $\sum_{|n|>\frac{R}{2\pi}} \frac{1}{(2\pi|n|-R)^2} < +\infty$, 故此级数在 K 上按范数收敛 (从而特别在所有点都收敛). 以 $f(z)$ 记此级数的和. 因为每个 $\frac{1}{(z+2i\pi n)^2}$ 在 $\mathbf{C} - 2i\pi\mathbf{Z}$ 上全纯, 故由定理 V.5.1 知 f 在 $\mathbf{C} - 2i\pi\mathbf{Z}$ 上全纯. 然而它与全纯函数 $z \mapsto \frac{e^z}{(e^z-1)^2}$ 在 $\mathbf{R}_+^*$ 重合. 由于 $\mathbf{C} - 2i\pi\mathbf{Z}$ 连通, 由孤立零点定理得到, 对于所有 $z \in \mathbf{C} - 2i\pi\mathbf{Z}$ 有 $f(z) - \frac{e^z}{(e^z-1)^2} = 0$.

习题 H.1.7. (i) 因为 $z \mapsto e^{\lambda z}$ 全纯且全纯函数的线性组合仍全纯, 故 $z \mapsto \cosh \pi z$ 亦如此. 其导数等于 $\pi \sinh \pi z$.

我们有 $\cosh \pi z = 0$ 当且仅当 $e^{\pi z} = -e^{-\pi z}$, 这等价于 $e^{2\pi z} = -1$, 从而等价于 $z = \frac{i}{2} + ki, k \in \mathbf{Z}$.

[563] (ii) 函数 f_u 在 $\mathbf{C}$ 上亚纯, 且在 $\frac{i}{2} + ki (k \in \mathbf{Z})$ 上有单极点. 现在有 $I(\gamma_R, \frac{i}{2} + ki) = 0, k \neq 0$, 而 $I(\gamma_R, \frac{i}{2}) = 1$. 由此并用留数公式得到

$$I(R) = 2i\pi \mathrm{Res}(f_u, \frac{i}{2}) = 2i\pi(e^{-2i\pi u \frac{i}{2}} \frac{1}{\pi \sinh \pi \frac{i}{2}}) = 2e^{\pi u}.$$

(iii) 当 $R \to +\infty$ 时, $\int_{[-R,R]} f_u(z)dz \to \hat{g}_1(u)$. 由于 $f_u(z+i) = -e^{2\pi u} f_u(z)$, 于是当 $R \to +\infty$ 时, 得到 $\int_{[R+i,-R+i]} f_u(z)dz = e^{2\pi u}\int_{[-R,R]} f_u(z)dz$ 趋向 $e^{2\pi u}\hat{g}_1(u)$. 最后, 在 $[R, R+i]$ 和 $[-R+i, -R]$ 上有 $|e^{-2i\pi uz}| \leqslant e^{2\pi u}$ 和 $|\frac{1}{\cosh \pi z}| \leqslant \frac{2}{e^{\pi R}-e^{-\pi R}}$; 由此得到 $\int_{[R,R+i]} f_u(z)dz$ 和 $\int_{[-R+i,-R]} f_u(z)dz$ 的模都被 $\frac{2e^{2\pi u}}{e^{\pi R}-e^{-\pi R}}$ 囿于上, 因此当 $R \to +\infty$ 时, 趋向 0. 于是得到 $I(R) \to (1+e^{2\pi u})\hat{g}_1(u)$, 而对所有的 $R > 0$ 有 $I(R) = 2e^{\pi u}$, 从而得到 $\hat{g}_1(u) = \frac{2e^{\pi u}}{1+e^{2\pi u}} = \frac{1}{\cosh \pi u}$.

$y>0$ 的情形可以通过伸缩公式 $(\mathscr{F}(f(ty))(x)=\frac{1}{y}\hat{f}(\frac{x}{y}))$ 得到.

(iv) 如果 $a>0$ 且 $z\in\Omega_a$, 则有 $|\frac{1}{\cosh\pi nz}|\leqslant\frac{2}{e^{\pi|n|a}-e^{-\pi|n|a}}$; 由此得知该级数在 Ω_a 上按范数收敛, 从而它的和 $F(z)$ 是 Ω_a 上的一个全纯函数. 因此它也在 $\Omega_0=\cup_{a>0}\Omega_a$ 上全纯.

现在, 如果 $y>0$, 则 $t\mapsto\frac{1}{\cosh\pi yt}$ 在 $\mathbf{R}$ 上可和, 其导数 $t\mapsto\frac{-\pi y\sinh\pi yt}{\cosh^2\pi yt}$ 也可和. 因此我们可对其应用泊松公式, 再利用 (iii), 便给出了恒等式 $\sum_{n\in\mathbf{Z}}\frac{1}{\cosh\pi yn}=\frac{1}{y}\sum_{n\in\mathbf{Z}}\frac{1}{\cosh\pi\frac{n}{y}}$, 它可以在此化为形如 $F(y)=\frac{1}{y}F(\frac{1}{y})$ 的公式.

最后, 在 Ω_0 上全纯的函数 $z\mapsto zF(z)-F(\frac{1}{z})$, 在 $\mathbf{R}_+^*$ 上为零; 因而根据孤立零点定理, 在连通开集 Ω_0 上恒等于零.

习题 H.1.8. (i) 由于由线段 $[0,R]$, 中心为 0 的从 R 走到 $e^{i\theta}R$ 的圆弧以及线段 $[e^{i\theta}R,0]$ 组成的道路是一个闭道, 于是根据留数定理有

$$I_1(R)+I_2(R)+I_3(R)=2i\pi(\sum_{a^n+1=0}I(\gamma_R,a)\mathrm{Res}(\frac{1}{z^n+1},a)).$$

$a^n+1=0$ 的解是 $e^{i\pi(2k+1)/n}$, 其中 $k\in\{0,1,\ldots,n-1\}$, 并且 $\frac{1}{z^n+1}$ 的每个极点都是单的; 因而它的留数是 $\frac{1}{na^{n-1}}=\frac{-a}{n}$. 另外, 指标 $I(\gamma_R,e^{i\pi(2k+1)/n})$ 当 $0<\frac{(2k+1)\pi}{n}<\theta$ 时为 1, 其他情形为 0. 因此有

$$I_1(R)+I_2(R)+I_3(R)=\frac{-2i\pi}{n}\sum_{0<\frac{(2k+1)\pi}{n}<\theta}e^{i\pi(2k+1)/n}.$$

(ii) 作为在 $\mathbf{R}_+$ 上可和的函数 $\frac{1}{1+t^n}$ 和 $\frac{1}{1+t^ne^{in\theta}}$, 我们有 $I_1(R)\to\int_0^{+\infty}\frac{dt}{1+t^n}$ 和 $I_3(R)\to-e^{i\theta}\int_0^{+\infty}\frac{dt}{1+t^ne^{in\theta}}$. 现在, $I_2(R)=\int_0^{\theta}\frac{iRe^{it}dt}{1+R^ne^{int}}$, 而 $|\frac{iRe^{it}}{1+R^ne^{int}}|$ 由 $\frac{R}{R^n-1}$ 囿于上. 因此 $|I_2(R)|\leqslant\frac{\theta R}{R^n-1}$, 由于 $n\geqslant 2$, 故证明了 $I_2(R)\to 0$.

(iii) 取 $\theta=\frac{2\pi}{n}$. 对 (i) 中的公式取极限得到

$$(1-e^{2i\pi/n})\int_0^{+\infty}\frac{dt}{1+t^n}=\frac{-2i\pi}{n}e^{i\pi/n},$$

从而有

$$\int_0^{+\infty}\frac{dt}{1+t^n}=\frac{2i\pi e^{i\pi/n}}{n(e^{2i\pi}/n-1)}=\frac{\pi/n}{\sin(\phi/n)}.$$

习题 H.1.9. (i) 函数 $z\mapsto\tan z$ 在 $\cos z$ 的零点之外全纯. 由于圆盘 $D(0,(\frac{\pi}{2})^-)$ 不包含任一个这种零点, 故 $\tan z$ 在整个圆盘上是其在 0 的泰勒级数的和 (注记 V.4.9 的 (i)), 因而在 $]-\frac{\pi}{2},\frac{\pi}{2}[$ 更是如此.

(ii) 函数 $z\mapsto\frac{\sin\pi z}{z-1}$ 除了在 $z=1$ 外全纯, 而在 $z=1$ 可能有一个一阶极点, 但在 $z=1$ 函数 $\sin\pi z$ 取零; 因此 $\frac{\sin\pi z}{z-1}$ 在整个 $\mathbf{C}$ 上全纯. 它在 0 的泰勒级数的收敛半径因此为 $+\infty$. [564]

习题 H.1.10. (i) 在 $D(0,R^-)$ 上有 $|\frac{z^2}{n^2}| \leqslant |\frac{R^2}{n^2}|$, 且由于 $\sum_{n\geqslant 1}\frac{R^2}{n^2} < +\infty$, 此乘积在 $D(0,R^-)$ 上绝对收敛. 它的每一项都全纯, 从而按照定理 V.5.4, 此乘积也全纯. 由此得到, 如此构造的函数 $z \mapsto F(z)$ 在 $\mathbf{C} = \cup_{R>0} D(0,R^-)$ 上全纯.

(ii) $\frac{1}{\sin \pi z}$ 在 $\mathbf{C}$ 上亚纯, 除了在整数的单极点外全纯并不取零. 另外, 由定理 V.5.4 知函数 F 的零点在非零整数上, 且为单零点. 由此得到, $z \mapsto \pi z F(z)$ 的零点在所有整数上且为单零点, 这表明它们恰好抵消了 $\frac{1}{\sin \pi z}$ 的极点, 从而 $G(z)$ 在 $\mathbf{C}$ 上全纯且不取零. 最后, 由于 $z \mapsto \sin \pi z$ 和 $z \to \pi z$ 都是奇函数, 故 G 是个偶函数.

(iii) 由于 $\mathbf{C}$ 可缩, 而 G 在 $\mathbf{C}$ 上全纯且不取零, 故根据命题 VI.2.3, 存在在 $\mathbf{C}$ 上的全纯函数 h 使得 $e^h = G$.

现在, 根据注记 V.4.9 的 (i), h 在整个 $\mathbf{C}$ 上是它在 0 的泰勒级数 $\sum_{n\in\mathbf{N}} a_n z^n$ 的和. 最后, 因 $F(0) = 1$ 且 $\lim_{z\to 0}\frac{\sin \pi z}{\pi z} = 1$, 故 $G(0) = 1$, 从而 $h(0) = a_0 \in 2i\pi\mathbf{Z}$. 由此得到, 如果 $g(z) = h(z) - a_0 = \sum_{n\geqslant 1} a_n z^n$, 则也有 $G = e^g$. 故有结论.

(iv) 根据最大值原理, C_N 是 $|G(z)|$ 在这个正方形边界上的最大值. 由于 G 为偶函数, 我们只需研究 $|G(z)|$ 在线段 $[(N+\frac{1}{2})(1-i),(N+\frac{1}{2})(1+i)]$ 和 $[(N+\frac{1}{2})(1+i),(N+\frac{1}{2})(i-1)]$ 上的值即可.

按照陈述中给出的下界, 在这些线段上有 $|\frac{1}{\sin \pi z}| \leqslant 1$. 将 $|\pi z|$ 以 πR_N 囿于上, 那么当 $n \leqslant N$ 时每个 $|1-\frac{z^2}{n}|$ 被 $1+|z|^2 \leqslant R_N^2+1$ 囿于上, 而当 $n \geqslant N+1$ 时则被 $1+\frac{|z|^2}{n^2} \leqslant e^{|z|^2/n^2}$ 囿于上. 于是便得到了我们希望得到的 C_N 的上界.

由于 $\sum_{n\geqslant N+1}\frac{1}{n^2} \leqslant \sum_{n\geqslant N+1}(\frac{1}{n-1}-\frac{1}{n}) = \frac{1}{N}$, 我们得到 $\log C_N \leqslant N\log(R_N^2+1)+\frac{R_N^2}{N}+\log \pi R_N$, 而因为 $R_N = O(N)$, 故 $\log C_N = O(N\log N)$, 得到结论.

(v) 我们有 $\mathrm{Re}(g(re^{i\theta})) = \mathrm{Re}(\sum_{n\geqslant 1}|a_n|r^n e^{i(n\theta+\alpha_n)}) = \sum_{n\geqslant 1}|a_n|r^n\cos(n\theta+\alpha_n)$. 由此得出 $I_n(r) = \sum_{n\geqslant 1}|a_n|r^n\int_0^{2\pi}(1+\cos(k\theta+\alpha_k))\cos(n\theta+\alpha_n)d\theta = \pi|a_k|r^k$. (可以用此级数在 $[0,2\pi]$ 上的按范数收敛性得到级数求和与积分的可交换性.)

另外, $\mathrm{Re}(g(re^{i\theta})) = \log|G(re^{i\theta})| \leqslant \log C_N, N = [r]+1$. 由此, 并因为 $0 \leqslant 1+\cos(k\theta+\alpha_k) \leqslant 2$, 得到囿于上的不等式 $I_N(r) = \int_0^{2\pi}(1+\cos(k\theta+\alpha_k))\mathrm{Re}(g(re^{i\theta}))d\theta \leqslant 2\log C_N$.

因此得到, 对于所有 $r>0$, 有囿于上的不等式 $|a_k| \leqslant \frac{2}{\pi}\frac{\log C_{[r]+1}}{r^k} = \frac{2}{\pi}\frac{\log C_{[r]+1}}{([r]+1)^k}\frac{([r]+1)^k}{r^k}$, 根据 (iv), 当 $k \geqslant 2$ 时, 它趋向 0. 得到结论.

(vi) 由 (iv) 和 (v) 得到 $G(z) = e^{a_1 z}$, 且由于 G 为偶函数, 故有 $a_1 = 0$, 从而 $G = 1$, 因此 $F(z) = \frac{\sin \pi z}{\pi z}$. 即为所证.

习题 H.1.11. (i) 函数 $s \mapsto \Gamma(s)\Gamma(1-s)$ 除了在所有整数上的单极点外全纯, 并因为 $s \mapsto \sin \pi s$ 在整数有零点, 这表明 F 在 $\mathbf{C}$ 上全纯. 现在有 $F(s+1) = (\sin \pi(s+1))\Gamma(s+1)\Gamma(-s) = (-\sin \pi s)(s\Gamma(s))(\frac{\Gamma(1-s)}{-s}) = F(s)$.

(ii) 由于 $\frac{\log z}{2i\pi}$ 在差一个整数的加法因子外有确定的定义, 而由于 F 是一个周期为 1 的周期函数, 故 $F(\frac{\log z}{2i\pi})$ 不依赖于 $\log z$ 的选取; 记其为 $f(z)$. 如果 $z_0 \in \mathbf{C}^*$, 我们

则可选定一个在 $D(z_0,|z_0|^-)$ 上全纯的对数 h (例如, 去掉半直线 $\mathbf{R}_+(-z_0)$ 得到). 因此在 $D(z_0,|z_0|^-)$ 上有 $f=F\circ h$, 这证明了 f 在 $D(z_0,|z_0|^-)$ 上全纯. 它对于所有的 $z_0\in\mathbf{C}^*$ 都成立, 故由此得到 f 在 $\cup_{z_0\in\mathbf{C}^*}D(z_0,|z_0|^-)=\mathbf{C}^*$ 上全纯.

(iii) 将推论 VI.3.2 应用于 $z_0=0, R_1=0$ 和 $R_2=+\infty$ 便得到了 a_n 的存在性. 另外, 根据此推论有 $a_n=\frac{1}{2i\pi}\int_{C(0,r)}z^{-n-1}f(z)dz, r>0$. 现在, 设 $\varphi:\mathbf{C}\to\mathbf{C}^*$ 由 $\varphi(s)=e^{2i\pi s}$ 定义. 按照习题 V.4.5, 对任意的连续函数 $g:\mathbf{C}^*\to\mathbf{C}$ 有 $\int_{[iT,1+iT]}(g\circ\varphi)\varphi'(s)ds=\int_{\varphi([iT,1+iT])}g(z)dz$. 因为 $\varphi([iT,1+iT])=C(0,r), r=e^{-2\pi T}$. 故对于 $g(z)=z^{-n-1}f(z)$ 我们得到恒等式 $a_n=\frac{1}{2i\pi}\int_{[iT,1+iT]}e^{-(n+1)2i\pi s}F(s)(2i\pi e^{2i\pi s})ds=\int_{[iT,1+iT]}e^{-2i\pi ns}F(s)ds$, 这就是我们想要的. [565]

(iv) 由于 F 和 $\mathrm{Im}(s)$ 为周期为 1 的周期函数, 故只需证明 G 在一个宽为 1 的一条竖直带 (譬如 $B=\{s,1\leqslant\mathrm{Re}(s)\leqslant 2\}$) 中有解即可, 而因为 G 连续, 它在紧集 $K=\{s\in B,|\mathrm{Im}(s)|\leqslant 1\}$ 上有界, 故只要证明 G 在 $B-K$ 上有界即可. 但 $\Gamma(s)$ 在 B 上有界, 而由于 $\Gamma(1-s)=\frac{\Gamma(3-s)}{(1-s)(2-s)}$, 且当 $s\in B$ 时 $3-s\in B$, 由此得到 $\Gamma(1-s)$ 也在 $B-K$ 上有界. 最后, $|\sin\pi s|\leqslant\frac{1}{2}(e^{\pi|\mathrm{Im}(s)|}+e^{-\pi|\mathrm{Im}(s)|})\leqslant e^{\pi|\mathrm{Im}(s)|}$. 因此有结果.

(v) 按照 (iv), 存在 $C>0$ 使得当 $s\in[iT,1+iT]$ 时有 $|e^{-2i\pi ns}F(s)|\leqslant Ce^{2\pi nT+\pi|T|}$. 由此, 对于 $T\in\mathbf{R}$ 有囿于上的不等式 $|a_n|\leqslant Ce^{2\pi nT+\pi|T|}$. 那么, 当 $n\geqslant 1$ (分别地, $n\leqslant -1$) 时让 T 趋向 $-\infty$ (分别地, $+\infty$), 便得到当 $n\neq 0$ 时有 $a_n=0$. 因此 f 为常值; 于是 F 也如此, 并由于 $F(0)=\lim_{s\to 0}\frac{\sin\pi s}{s}\Gamma(s+1)\Gamma(1-s)=\pi$, 得到结论.

习题 H.1.12. (i) 根据柯西不等式 (注记 V.4.9 的 (i)), 有 $|g'(z_0)|\leqslant\frac{1}{r}\sup_{z\in C(z_0,r)}|g(z)|$, 其中 $z_0=x_0+iy_0$. 如果 $|y_0|\geqslant M'=2M$, 且 $r=\frac{|y_0|}{2}$, 则有 $M\leqslant|\mathrm{Im}(z)|\leqslant\frac{3|y_0|}{2}$, 其中 $z\in C(z_0,r)$, 因此有 $|g(z)|\leqslant C(\frac{3|y_0|}{2})^N$. 由此得到, 当 $|y_0|\geqslant M'$ 时有 $|g'(z_0)|\leqslant C'|y_0|^{N-1}$, 其中 $C'=3^N2^{1-N}$.

(ii) 令 $g=f^2+f'$. 由于 f 在 $D(0,1^-)-\{0\}$ 上全纯, 且为奇函数, 并有留数为 1 的在 0 的单极点, 故在 $D(0,1^-)$ 上有 $f(z)=\frac{1}{z}+\sum_{n=0}^{+\infty}a_{2k+1}z^{2k+1}$ (在一个有孔圆盘上的全纯函数, VI.3 的 2 小节). 由此推出 $f'(z)=\frac{-1}{z^2}+\sum_{n=0}^{+\infty}(2k+1)a_{2k+1}z^{2k}$ 以及 $f(z)^2=\frac{1}{z^2}+2a_1+\cdots$, 因此 $g(z)$ 在 0 全纯. 由于它是周期为 1 的周期函数, 它在所有整数上全纯, 并由于 f 在 $\mathbf{C}-\mathbf{Z}$ 上全纯, 故它在整个 $\mathbf{C}$ 上全纯.

又, 从 (i) 得知 g 是一个 $O(y^{2N})$ 且对所有的 k, $g^{(k)}$ 是一个 $O(y^{2N-k})$. 由此推出 $g^{(2N)}$ 在 $\{z,0\leqslant\mathrm{Re}(z)\leqslant 1,|\mathrm{Im}(z)|\geqslant M_N\}$ 上有界, 其中 M_N 充分大. 因为 $g^{(2N)}$ 在 $\{z,0\leqslant\mathrm{Re}(z)\leqslant 1\}$ 上连续 (由于全纯), 而 $\{z,0\leqslant\mathrm{Re}(z)\leqslant 1,|\mathrm{Im}(z)|\leqslant M_N\}$ 为紧集, 故存在 C_N 使得当 $0\leqslant\mathrm{Re}(z)\leqslant 1$ 时有 $|g^{(2N)}(z)|\leqslant C_N$; 由刘维尔定理得到 $g^{(2N)}$ 为常值. 故推出 g 是一个次数 $\leqslant 2N$ 的多项式, 又由于 g 为周期函数, 因此 g 是常数, 结论得证.

我们也可得到 $h(z)=f(z)-\pi\cot\pi z$ 是在 $\mathbf{C}$ 上全纯的、奇的、周期为 1 的周期函数, 并且是 $O(y^N)$ 的. 如上面同样的推理还可证明 $h=0$, 从而 $f^2+f'=-\pi^2$.

习题 H.1.13. (i) 设 $\Omega' = \{z \in \Omega, |f(z) - g(z)| < |f(z)|\}$. 则 Ω' 作为 $\mathbf{R}^2$ 中开集 $\{(x,y), x < y\}$ 在连续映射 $z \mapsto (|f(z)-g(z)|, |f(z)|)$ 下的逆像是个开集, 并按假设条件, Ω' 包含了 C. 现在, 如果 $z \in \Omega'$, 我们有 $|\frac{g(z)}{f(z)} - 1| < 1$, 它让我们将 h 定义为 $\frac{g}{f} : \Omega' \to D(1, 1^-)$ 和 $\log : D(1,1^-) \to \mathbf{C}$ 的复合, 其中 log 是对数的主分支. 因此有 $h' = \frac{(e^h)'}{e^h} = \frac{(g/f)'}{g/f} = \frac{g'}{g} - \frac{f'}{f}$.

(ii) 函数 $\frac{f'}{f} - \frac{g'}{g}$ 以 $-h$ 为其在 Ω' 上的原函数, 从而在包含在 Ω' 中的整个闭道上的积分为零. 特别地, $\int_C (\frac{f'(z)}{f(z)} - \frac{g'(z)}{g(z)}) dz = 0$ (其中沿 C 的正方向). 利用命题 VI. 3.14(因为按假设条件 f 在 C 上不取零, 而由于当 $z \in C$ 时 $|f(z) - g(z)| < |f(z)|$, 故 g 也不取零) 得知 f 和 g 在 D 中有相同个数的零点 (计入重数).

(iii) D 为紧集而 G 在 D 上连续, 故存在 $z_0 \in D$ 使得 $|G|$ 在 z_0 达到其最大值, 而最大值原理表明 $z_0 \in C$. 由于按假设 $|G(z_0)| < 1$, 故当 $z \in D$ 时有 $|G(z)| < 1$, 从而 $G(D) \subset D$. 将 (ii) 用到 $f(z) = z, g(z) = z - G(z)$, 由此推出 f 和 g 在 D 中的零点的个数相同, 但 f 有唯一的在 0 的零点, 故表明 g 有唯一的零点, 从而 G 在 D 中有唯一的不动点.

[566] **习题 H.1.14.** (i) 如果 $a > 1$ 而 $\mathrm{Re}(s) > a$, 则除了使得 $|n + x| < 1$ 的 n 的有限集合外, 我们有 $|\frac{1}{(n+x)^s}| \leqslant \frac{1}{(n+x)^a}$. 由于 $\sum_{n=0}^{+\infty} \frac{1}{(n+x)^a} < +\infty$, 故级数 $\sum_{n\in\mathbf{N}} \frac{1}{(n+x)^s}$ 在 $\mathrm{Re}(s) > a$ 上按范数收敛. 由定理 V.5.1 的 (ii) 知, 这个级数的和 $F(x,s)$ 在 $\mathrm{Re}(s) > a$ 上全纯. 这对所有 $a > 1$ 为真, 故 $F(x,s)$ 在 $\mathrm{Re}(s) > 1$ 上全纯.

(ii) 我们有 $\frac{1}{(n+x)^s} = \frac{1}{\Gamma(s)} \int_0^{+\infty} e^{-(n+x)t} t^{s-1} dt$, 其中 $\mathrm{Re}(s) > 0$. $\sum_{n=0}^{+\infty} e^{-(n+x)t} t^{s-1}$ 的部分和的绝对值被 $\sum_{n=0}^{+\infty} e^{-(n+x)t} t^{\mathrm{Re}(s)-1} = \frac{te^{-tx}}{1-e^{-t}} t^{\mathrm{Re}(s)-2}$ 囿于上, 并由于在 $+\infty$ 速降且在 0 等价于 $t^{\mathrm{Re}(s)-2}$, 故它当 $\mathrm{Re}(s) - 2 > -1$ 时可和, 那么, 如果 $\mathrm{Re}(s) > 1$, 利用控制收敛定理交换求和与积分便得到

$$
\begin{aligned}
F(x,s) &= \sum_{n=0}^{+\infty} \frac{1}{\Gamma(s)} \int_0^{+\infty} e^{-(n+x)t} t^{s-1} dt \\
&= \frac{1}{\Gamma(s)} \int_0^{+\infty} \sum_{n=0}^{+\infty} e^{-(n+x)t} t^{s-1} dt \\
&= \frac{1}{\Gamma(s)} \int_0^{+\infty} \frac{e^{-tx}}{1-e^{-t}} t^{s-1} dt.
\end{aligned}
$$

(iii) 令 $g_x(t) = \frac{te^{-tx}}{1-e^{-t}}$. 于是作为在 $2i\pi\mathbf{Z} - \{0\}$ 外的一个全纯函数的限制的 g_x 在 $\mathbf{R}_+$ 上为 $\mathscr{C}^\infty$ 的, 并与它的所有阶导数在无限远速降. 因此它满足应用命题 VII.2.6 的条件, 从而 $M(g_x, s) = \frac{1}{\Gamma(s)} \int_0^{+\infty} \frac{te^{-tx}}{1-e^{-t}} t^{s-1} dt$ 具有一个到 $\mathbf{C}$ 的并满足 $M(g_x, 0) = g_x(0) = 1$ 的全纯延拓, 然而我们有 $\Gamma(s) = (s-1)\Gamma(s-1)$, 因此 $F(x,s) = \frac{1}{s-1} M(g_x, s-1)$. 得到结果.

H.2. A_5 的特征标表 [567]

本问题的目标是建立称作二十面体群的 60 阶群 A_5 的特征标表 (图 4).

		1	χ_U	χ_V	χ_W	$\chi_{W'}$
1	C_1	1	4	5	3	3
20	C_3	1	1	-1	0	0
15	$C_{2,2}$	1	0	1	-1	-1
12	C_5	1	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
12	C'_5	1	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$

图 4. A_5 的特征标表

我们将利用以下没有证明过的事实:

- 如果 i, j, k(分别地, i', j', k') 是 $\{1, 2, \ldots, 5\}$ 中不同的元, 则存在 $g \in A_5$ 使得 $g(i) = i', g(j) = j'$ 和 $g(k) = k'$ (事实上 g 是唯一的).
- 群 A_5 有 5 个共轭类[4]:

  — 中性元的类 C_1, 基数为 1.

  — 3-循环的类 (3 阶), 基数为 20.

  — 两个具有不交支集的对换的乘积 (2 阶), 基数为 15.

  — 基数为 12 的两个类 C_5 和 C'_5, 它们的并是 5-循环 (5 阶) 的集合. 另外, 如果 t [568] 是一个 5-循环, 则 t 和 t^2 不在同一个类中. 为了确定起见, 我们以 C_5 记 $t_0 = (12345)$ 的类, 而 C'_5 为 $t_0^2 = (13524)$ 的类.

问题 1. (a) 证明 A_5 有 5 个不可约表示, 且其中至少有一个是 1 维的.

---

[4] A_5 的共轭类可以从 S_5 的共轭类推出. 温习一下: 如果 G 是一个群, 而 $x \in G$, Z_x 是 x 的中心化子 (即 G 中与 x 交换的元的集合), 则 x 的共轭类经 $g \mapsto gxg^{-1}$ 同构于 G/Z_x; 特别地, 它的基数等于 $\frac{|G|}{|Z_x|}$. 为了了解 S_5 中的一个共轭类在 A_5 中是什么, 涉及了解 x 在 S_5 中的中心化子 Z_x 与它在 A_5 中的中心化子 $Z_x \cap A_5$ 的位置. 但 A_5 是符号差 $\varepsilon : S_5 \to \{\pm 1\}$ 的核, 由此知, 如果 H 是 S_5 的一个子群, 则要么 $H \subset A_5$ 要么 $\varepsilon : H \to \{\pm 1\}$ 为满射, 从而 $H \cap A_5$ 作为它的核, 其基数为 $|H|/2$. 设 $C \in \mathrm{Conj}(S_5)$. 如果 $C \cap A_5 \neq \emptyset$, 则 S_5 的特征标 ε 在 C 的某个元上取 1, 从而在整个 C 上取 1; 换言之, $C \subset A_5$. 现在, 如果 $x \in C$, 在 A_5 中 x 的共轭类 C_x 包含在 C 中, 而如果 Z_x 是其在 S_5 中的中心化子, 则可分为两种情形:

- $Z_x \subset A_5$, 于是 $|C_x| = \frac{|A_5|}{|Z_x|} = \frac{1}{2}\frac{|S_5|}{|z_x|} = \frac{1}{2}|C|$, 从而 C 分裂成 A_5 中的两个共轭类.
- Z_x 包含了一个符号差为 -1 的元, 从而 $|Z_x \cap A_5| = \frac{1}{2}|Z_x|$, 它表明 C_x 的基数为 $\frac{|A_5|}{|Z_x \cap A_5|} = \frac{|S_5/2|}{|Z_x|/2} = \frac{|S_5|}{|Z_x|} = |C|$ 以及 $C_x = C$ 和 C 是 A_5 的一个共轭类.

由于 (45) 与 (123) 交换, 则这些 3-循环是 A_5 的共轭类. 同样, (12) 与 (12)(34) 交换, 从而 $C_{2,2}$ 是 A_5 的一个共轭类. 相反地, 5-循环的个数为 24, 而 24 不能整除 $|A_5| = 60$, 这表明 5-循环的类在 A_5 中分裂为两个. 由于 $(13524) = \sigma(12345)\sigma^{-1}$, 其中 $\sigma = (2354)$, 而 $\varepsilon(\sigma) = -1$, 从而得到 $t_0 = (12345)$ 和 t_0^2 不在 A_5 的同一个等价类中, 并因为这些 5-循环全都在 S_5 中共轭, 这便证明了对于每个 5-循环 t, t 与 t^2 都不在 A_5 的同一个共轭类中.

(b) 证明这些不可约表示的维数分别是 $1, 3, 3, 4$ 和 5.

(c) 那个一维表示是什么? 以 U 记其中的 4 维的表示, V 为 5 维的, 而 W 和 W' 是 3 维的. 我们可以从上面得到这个表格的哪一部分?

问题 2. 以 T 记由 A_5 的特征标表定义的 5×5 矩阵.

(a) 证明 TT^* 是系数为 $60, 3, 4, 5, 5$ 的对角矩阵 (利用注记 I.2.35).

(b) 由此推出 $|\chi(g)|$ 的一个囿于上的函数, 然后推出对所有的 $\chi \in \mathrm{Irr}(A_5) - \{1\}$ 和 $g \neq 1$ 有 $|\chi(g)| \neq |\chi(1)|$.

(c) 由此推出 A_5 为单群 (回顾, 如果 G 非单, 则存在一个满的群态射 $f: G \to H, H \neq \{1\}$ 使得其核不退化为 $\{1\}$).

问题 3. 设 U' 是 A_5 相伴于 A_5 在 $\{1, \ldots, 5\}$ 上的自然作用 (即 $g(e_i) = e_{g(i)}$, 其中 $g \in A_5, i \in \{1, \ldots, 5\}$) 的置换表示, 并设 U 是方程 $x_1 + \cdots + x_5 = 0$ 定义的 U' 中的超平面.

(a) 计算 $g \cdot x$, 其中 $x = (x_1, \ldots, x_5), g \in A_5$, 并证明 U 在 A_5 下稳定.

(b) 设 $x \in U$. 证明 U 的由 $g \cdot x (g \in A_5)$ 生成的子空间 U_x 在 A_5 下稳定, 并且包含了一个三个坐标为零的非零向量 (由考虑形如 $g \cdot x - x$ 的元先证明它包含一个两个坐标为零的非零向量).

(c) 由此推出 U 不可约.

(d) 计算 U 和 U' 的特征标; 重证 U 不可约.

问题 4. (a) 设 Y 是 A_5 的一个表示. 证明 $g \mapsto \det \rho_Y(g)$ 是 A_5 的一个特征标. 由此推出对于所有 $g \in A_5$ 有 $\det \rho_Y(g) = 1$.

(b) 填写 T 的最后两列的前两行. (考虑 A_5 的 3 维不可约表示 Y, 它涉及 ρ_Y 的特征值 λ_1, λ_2 和 λ_3. 并利用问题 2 的 (b).)

(c) 证明 C_5 和 C_5' 在 $g \mapsto g^{-1}$ 下稳定, 由此推出, 如果 g 是个 5-循环, 则 $\rho_Y(g)$ 的这些特征值在 $\lambda \mapsto \lambda^{-1}$ 下整体稳定.

(d) 完成 T 的最后两列的填写. (利用公式 $\cos \frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$ 和 $\cos \frac{4\pi}{5} = \frac{-\sqrt{5}-1}{4}$.)

(e) 如何完成 A_5 的特征标表?

问题 5. 设 Y 是 A_5 在 $\{1, \ldots, 5\}$ 的 10 个不同偶对的集合上作用相伴的置换表示. 计算 Y 的特征标 χ_Y 以及标量积 $\langle \chi_Y, \mathbf{1} \rangle$ 和 $\langle \chi_Y, \chi_U \rangle$, 并由此得出计算 χ_V 的另一种方法.

问题校正

[569]

问题 1. (a) 根据推论 I.2.16, $\mathbf{A}_5$ 的不可约表示的个数等于它的共轭类的个数, 即 5. 另外, 每个群都有以平凡表示 (1 维) 作为的不可约表示.

(b) 根据 Burnside 公式, 如果 d_2, d_3, d_4, d_5 代表不是平凡的那些表示的维数, 于

是有 $1+d_2^2+d_3^2+d_4^2+d_5^2=|A_5|=60$, 或者说可以以唯一的方式 (在允许置换下) 将 59 写成 4 个数的平方和, 即 $59=5^2+4^2+3^2+3^2$. (这可通过一系列的研究看出; 而用 mod 8 则可以进行得更快一些, 用它可以证明 d_i 中有一个为 4(因为其余的 4 的倍数过大) 而另外的 d_i 为奇数.)

(c) 维数 1 的表示是平凡的, 并由于 $\chi(1)$ 是对应于 χ 的表示的维数, 故可填满特征标表的第一行和第一列.

问题 2. (a) 根据注记 I.2.35, TT^* 是在对应于 C 的行上的系数为 $|G|/|C|$ 的对角线矩阵. 因此此对角矩阵的系数为 $60/1=60, 60/20=3, 60/15=4, 60/12=5$ 和 $60/12=5$.

(b) TT^* 上对应于 C 类的行的对角线上系数也等于 $\sum_{\chi\in\mathrm{Irr}(A_5)}|\chi(C)|^2$. 由于当 $C\neq C_1$ 时这个系数 $\leqslant 5$, 那么按照 (a), 这证明当 $C\neq C_1$ 时, 对所有的 $\chi\in\mathrm{Irr}(A_5)$ 有 $|\chi(C)|<3$, 而由于如果 $\chi\in\mathrm{Irr}(A_5)-\{\mathbf{1}\}$, 有 $|\chi(1)|\geqslant 3$, 故得结论.

(c) 如果 A_5 不是单群, 则会存在一个满的群态射 $f: A_5\to H$, 其中 $H\neq\{1\}$, 而其核 $\mathrm{Ker}\, f\neq\{1\}$. 由于 $H\neq\{1\}$, 故存在 H 的不同于平凡表示的不可约表示 V (这从 Burnside 公式得到). 然而这样 $\rho_V\circ f$ 便是从 A_5 到 $\mathrm{GL}(V)$ 的一个群态射, 这让我们可以将 V 看成是 A_5 的一个表示. $v\in V$ 在 A_5 作用下的像同于在 H 作用下的像, 于是 A_5 的表示是不可约的, 从而有 $\chi_V(g)=\chi_V(1)$, 其中 $g\in\mathrm{Ker}\, f$. 这与 (b) 相矛盾, 因此有结论.

问题 3. (a) 我们有 $g\cdot(x_1e_1+\cdots+x_5e_5)=x_1e_{g(1)}+\cdots+x_5e_{g(5)}$, 因而 $g\cdot(x_1,\ldots,x_5)=(x_{g^{-1}(1)},\ldots,x_{g^{-1}(5)})$. 由此推出, $g\cdot x$ 的坐标与 x 的坐标在差一个置换下是一样的, 从而 x 和 $g\cdot x$ 的坐标和相等. 由此得到 U 在 A_5 的作用下稳定.

(b) U_x 在 A_5 下的稳定性来自 $h\cdot(g\cdot x)=hg\cdot x$, 因而 x 的平移的线性组合的平移仍是 x 的平移的线性组合.

设 $x=(x_1,\ldots,x_5)$. 由于 $x\in U$, 故存在 $i\neq j$ 使得 $x_i\neq x_j$. 必要时可用 $h\cdot x$ 替换 x, 其中 $h\in A_5$ 满足 $h(1)=i, h(2)=j$, 故不妨设 $i=1, j=2$. 设 $g=(132)$. 于是 $g\cdot x=(x_2,x_3,x_1,x_4,x_5)$ 而 $y=g\cdot x-x=(y_1,y_2,y_3,0,0)$, 其中 $y_1=x_2-x_1\neq 0$. 因为 $y\in U_x$, 便得到在 U_x 中存在一个其坐标有两个 0 的非零元 y.

由于 $y\in U_x$, 那么 y 的三个非零坐标不是全都相等的, 故存在 $i\neq j$ 使得 $y_i\neq y_j$. 像上面那样, 不妨设 $i=1, j=2$, 而 $y_4=y_5=0$. 令 $g'=(12)(45)$, 并令 $w=g'\cdot y-y$. 于是 $w\in U_x$, 且 $w=(y_2-y_1, y_1-y_2, 0,0,0)$ 非零但有三个坐标为零.

(c) 需要证明当 $x\in U$ 非零时, 由 $g\cdot x$ 生成的 U 的子空间 U_x 等于 U. 但根据 (b), U_x 包含了一个形如 $e_i-e_j (i\neq j)$ 的向量. 由于 $g\cdot(e_i-e_j)=e_{g(i)}-e_{g(j)}$, 且由于对所有 $i'\neq j'$ 存在 $g\in A_5$ 使得 $g(i)=i', g(j)=j'$, 故可以看出 U_x 包含了对所有偶对 $i\neq j$ 的 e_i-e_j. 特别包含了 U 中的 $e_i-e_1, 2\leqslant i\leqslant 5$, 故得结论.

(d) 由于 U' 是一个置换表示, 故 $\chi_{U'}(g)$ 是 $g\in A_5$ 作用在 $\{1,\ldots,5\}$ 上的不动点

的个数. 因此有 $\chi_{U'}(C_1)=5, \chi_{U'}(C_3)=2, \chi_{U'}(C_{2,2})=1, \chi_{U'}(C_5)=\chi_{U'}(C'_5)=0$.

[570] U' 的表示是 U 与由 $e_1+\cdots+e_5$ 生成的直线的直和, 其中 A_5 在后者的作用为平凡的. 因此 $\chi_{U'}(g)=\chi_U(g)+\chi_1(g)$, 其中对所有的 $g\in A_5$ 有 $\chi_U(g)=\chi_{U'}(g)-1$. 至于 $\chi_{U'}$ 的值, 它们给出了特征标表的第二列.

最后, $\langle\chi_U,\chi_U\rangle=\frac{1}{60}(4^2+20\cdot 1^2+15\cdot 0^2+12\cdot(-1)^2+12\cdot(-1)^2)=\frac{1}{60}(16+20+12+12)=1$, 这证明了 U 不可约 (推论 I.2.21).

问题 4. (a) 映射 $g\mapsto \det\rho_Y(g)$ 是从群 G 到 $\mathbf{C}^*$ 的一个态射, 它是态射 $g\mapsto\rho_Y$ 与 $u\mapsto\det u$ 的复合; 因此是 A_5 的一个线性特征标. 然而一个线性特征标必定定义了一个不可约的 1 维表示. 由于 A_5 只有唯一的 1 维的不可约表示 (即平凡表示) 从而得到结论.

(b) • 如果 g 是一个 3-循环, 则 $\rho_Y(g)^3=\rho_Y(g^3)=1$, 从而 $\lambda_1,\lambda_2,\lambda_3$ 是 3 次单位根, 又根据 (a), 它们的乘积等于 1, 并且由问题 2 的 (b) 知它们不全相等. 因此有 $\{\lambda_1,\lambda_2,\lambda_3\}=\{1,e^{2i\pi/3},e^{-2i\pi/3}\}$, 于是 $\chi_Y(g)=\lambda_1+\lambda_2+\lambda_3=0$, 这便填写进了 T 的最后两列的第 2 行.

• 如果 g 的阶为 2, 则 $\lambda_1,\lambda_2,\lambda_3$ 取值 ±1 且其中一个为 1, 而它们的乘积为 1. 因此其中有两个为 -1, 一个为 1. 于是得到 $\chi_Y(g)=\lambda_1+\lambda_2+\lambda_3=-1$, 它可填写进 T 的最后两列的第 3 行.

(c) $g\mapsto g^2$ 交换了 C_5 和 C'_5, 从而 $g\mapsto g^4$ 让 C_5 和 C'_5 稳定. 然而, 如果 g 是个 5-循环, 则因为 $g^5=1$, 故 $g^4=g^{-1}$.

因此, 如果 g 是个 5-循环, 则 g 和 g^{-1} 在同一个共轭类中, 故存在 $h\in A_5$ 使得 $g^{-1}=hgh^{-1}$. 这意味着 $\rho_Y(g)^{-1}=\rho_Y(g^{-1})=\rho_Y(h)\rho_Y(g)\rho_Y(h)^{-1}$, 从而 $\rho_Y(g)^{-1}$ 与 $\rho_Y(g)$ 具有相同的特征值 (计入重数). 由于 $\rho_Y(g)^{-1}$ 的特征值是 $\rho_Y(g)$ 的特征值的逆, 得到所要结论.

(d) 如果 $g\in C_5$, 则 $\rho_Y(g)$ 的特征值 $\lambda_1,\lambda_2,\lambda_3$ 为 5 次单位根, 并不全为 1, 根据 (c), 这个集合在 $\lambda\to\lambda^{-1}$ 下稳定. 因此有两种可能性: $\{\lambda_1,\lambda_2,\lambda_3\}=\{1,e^{2i\pi/5},e^{-2i\pi/5}\}$ 或 $\{\lambda_1,\lambda_2,\lambda_3\}=\{1,e^{4i\pi/5},e^{-4i\pi/5}\}$. 在第一种情形, 我们有 $\chi_Y(g)=\frac{1+\sqrt5}{2}$ 而在第二种情形有 $\chi_Y(g)=\frac{1-\sqrt5}{2}$. 另外, $g^2\in C'_5$, 而 $\rho_Y(g^2)$ 的特征值是 $\rho_Y(g)$ 的特征值的平方. 由此得到, 如果 $\chi_Y(C_5)=\frac{1+\sqrt5}{2}$, 则 $\chi_Y(C'_5)=\frac{1-\sqrt5}{2}$, 而如果 $\chi_Y(C_5)=\frac{1-\sqrt5}{2}$, 则 $\chi_Y(C'_5)=\frac{1+\sqrt5}{2}$. 由于 A_5 有两个 5 维的不可约表示, 并且其特征标决定了表示 (推论 I.2.19), 这表明这两种可能性都出现了. 得到结论.

(e) 只需利用正则分解 (推论 I.2.23); 它对于 $g\neq1$ 给出了公式 $1+4\chi_U(g)+5\chi_V(g)+3\chi_W(g)+3\chi_{W'}(g)=0$, 并由于我们除了 $\chi_V(g)$ 这一项外其余全已知, 因此得到结论.

问题 5. 由于 Y 是一个置换表示, 故 $\chi_Y(g)$ 是 $g\in A_5$ 作用于 $\{1,\ldots,5\}$ 的不同元的偶对的集合上的不动点的个数. 因为有 10 个这种偶对, 则有 $\chi_Y(C_1)=10$.

被 (123) 固定的唯一偶对是 $\{4,5\}$, 从而 $\chi_Y(C_3) = 1$. 在 (12)(34) 作用下不动的是 $\{1,2\}$ 和 $\{3,4\}$, 从而 $\chi_Y(C_{2,2}) = 2$. 最后, 没有任何偶对在 5-循环下稳定, 故 $\chi_Y(C_5) = \chi_Y(C_5') = 0$. 现在,

$$\langle \chi_Y, \mathbf{1} \rangle = \frac{1}{60}(10 + 20 \cdot 1 + 15 \cdot 2 + 12 \cdot 0 + 12 \cdot 0) = \frac{1}{60}(10 + 20 + 30) = 1,$$

$$\langle \chi_Y, \chi_U \rangle = \frac{1}{60}(40 + 20 \cdot 1 + 15 \cdot 0 + 12 \cdot 0 + 12 \cdot 0) = \frac{1}{60}(40 + 20) = 1.$$

由此推出 Y 可分解为 $\mathbf{1} \oplus U \oplus Y'$, 其中 Y' 是 5 维的并不包含于 $\mathbf{1}$ 或 U 的不可约分支. 由于剩余的那些不可约分支的维数为 5, 3, 3, 故由此看出 Y' 不可约, 同构于 V, 从而 $\chi_V = \chi_Y - \chi_U - \chi_{\mathbf{1}}$.

注记. [571]

我们可以从一个二十面体 (它是一个正多面体, 具有 12 个顶点, 从每个顶点出发有 5 条边, 它有 20 个面, 每个面是个等边三角形) 出发来几何地构造表示 W. 反过来, 费一点力气也可在 W 内部构造出一个 3 维 $\mathbf{R}$ 子空间 W_0, 它在 A_5 下稳定 (并使得 $W = W_0 \oplus iW_0$). 在 W 上取一个在 A_5 下不变的标量积 (参看定理 I.2.6), 它便赋予 W_0 一个使得 A_5 的作用是等距的 (甚至根据问题 4 的 (a), 是个旋转的) 标量积. 特别地, $t_0 = (12345)$ 的作用是个角为 $\pm\frac{2\pi}{5}$ 的旋转, 而如果 f 是这个旋转轴上的单位向量, 那么 f 的稳定化子是由 t_0 生成的 5 阶群, f 在 A_5 的作用下有 $60/5 = 12$ 个平移. 我们可以证明这些平移是一个二十面体的顶点 (图 5).

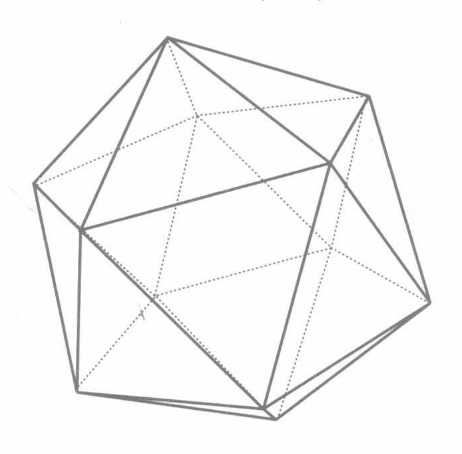


图 5. 二十面体

同样, 如果 f 是由 (123) 定义的角为 $\pm\frac{2\pi}{3}$ 的旋转轴的单位向量, 则 f 有 $60/3 = 20$ 个平移. 可以证明这些平移是一个十二面体 (图 6) 的顶点 (一个正多面体, 它具有 20 个顶点而每个顶点发出 3 条边, 并具有 12 个正五边形的面).

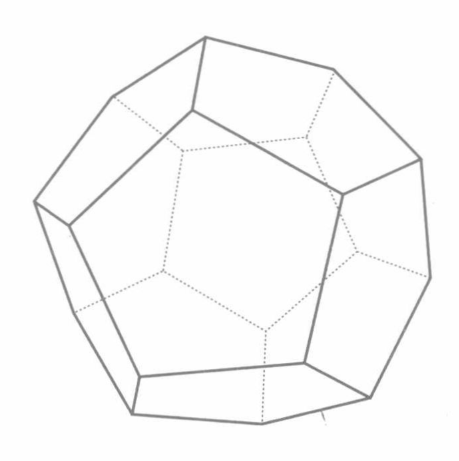


图 6. 十二面体

[572] H.3. $\mathbf{GL}_2(\mathbf{F}_3)$ 的表示

这个作业的目标是用逐次对 G 解套的方法[5] 构造群 $G = \mathbf{GL}_2(\mathbf{F}_3)$ 的特征标表，其中 $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z}$ 是有三个元的域 (一般地记为 0, 1 和 -1). 另一个解决方法在附录 C 中提出过.

群 G 是一个基数为 48 的群[6], 它作用于 $\mathbf{F}_3$-向量空间 $\mathbf{F}_3 \times \mathbf{F}_3$, 并由于其作用是线性的, 它将一条向量直线转换为向量直线; 因此作用在这些直线的空间 $\mathbf{P}^1(\mathbf{F}_3)$ 上, 一共有四个元: 分别由 $e_1, e_2, e_1 + e_2, e_1 - e_2$ 生成的直线 $\Delta_1, \Delta_2, \Delta_3, \Delta_4$, 其中 e_1, e_2 代表 $\mathbf{F}_3 \times \mathbf{F}_3$ 的 $\mathbf{F}_3$-标准基. 由此推出一个态射 $\sigma : G \to S_4$, 其定义为 $g \cdot \Delta_i = \Delta_{\sigma(g)(i)}$, 其中 $i \in \{1, 2, 3, 4\}$ (图 7).

	$\mathbf{1}$	ε	θ
1	1	1	2
(1, 2)	1	-1	0
(1, 2, 3)	1	1	-1

	$\mathbf{1}$	ε	θ	χ_1	χ_2
1	1	1	2	3	3
(1, 2)	1	-1	0	1	-1
(1, 2)(3, 4)	1	1	2	-1	-1
(1, 2, 3)	1	1	-1	0	0
(1, 2, 3, 4)	1	-1	0	-1	1

图 7. S_3 和 S_4 的特征标表

[5] 怀尔斯对费马大定理的证明, 基于两个不起眼但出乎意料的东西, 即这些解套的存在性以及 G 的表示 V 的存在性, 在此问题的构造中, 它是从群 G mod 3 的自然表示到特征 0 的一个提升: 它是 2 维的, 并在 $\rho_V(g)$ 的迹的 mod 3 约化是 g 的迹.

[6] 将 $g \in G$ 映到它的两个列向量的映射是从 G 到 $\mathbf{F}_3 \times \mathbf{F}_3$ 在 $\mathbf{F}_3$ 上的基族的集合间的一个双射. 由于一组基是由第一个非零向量与第二个不属于第一个向量生成的直线的向量, 故有 $|G| = (9-1)(9-3) = 48$.

我们将利用这个态射从我们承认的 S_4 的特征标表着手来构造 G 的特征标表 [7].

如果 $g=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in G$, 并以 $-g$ 记 G 的元 $\begin{pmatrix}-a&-b\\-c&-d\end{pmatrix}$. 记 G 的下列元为:

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},S=\begin{pmatrix}0&1\\1&0\end{pmatrix},D=\begin{pmatrix}0&1\\-1&0\end{pmatrix},T=\begin{pmatrix}1&1\\0&1\end{pmatrix},C=\begin{pmatrix}0&1\\1&1\end{pmatrix}.$$

问题 1. (i) 设 K 为域, 而 $g\in\mathbf{GL}_2(K)$ 不是一个位似矩阵.

(a) 证明存在 $v\in K^2$ 使得 v 和 $g(v)$ 构成 K^2 在 K 上的一组基.

(b) 由此推出 g 在 $\mathbf{GL}_2(K)$ 中的共轭类是 $\begin{pmatrix}0&-\det(g)\\1&\mathrm{Tr}(g)\end{pmatrix}$ 的共轭类. [573]

(ii) 验证图 8 中的 G 的共轭类列表是正确的 (列出 $\mathrm{Irr}(G)$ 的元的表示以替代特征标).

	$\mathbf{1}$	ε	U	V_1	V_2	W	V	V'
I	1	1	2	3	3	4	2	2
$-I$	1	1	2	3	3	-4	-2	-2
S	1	-1	0	1	-1	0	0	0
D	1	1	2	-1	-1	0	0	0
T	1	1	-1	0	0	1	-1	-1
$-T$	1	1	-1	0	0	-1	1	1
C	1	-1	0	-1	1	0	$i\sqrt{2}$	$-i\sqrt{2}$
$-C$	1	-1	0	-1	1	0	$-i\sqrt{2}$	$i\sqrt{2}$

图 8. $\mathbf{GL}_2(\mathbf{F}_3)$ 的特征标表

问题 2. (i) 证明 $\sigma:G\to S_4$ 的核为 $\{\pm I\}$, 且 σ 是满的.

(ii) 确定 $\sigma(g)$, 其中 $g\in\{I,-I,S,D,T,-T,C,-C\}$.

(iii) 从 S_4 的表示出发构造 G 的不可约表示中的 5 个. 表中的哪一列可以用它填写满?

问题 3. (i) 计算所缺少的不可约表示的个数和维数.

(ii) 证明, 如果 V 是 G 的一个表示, 则 $V^+=\{v\in V,(-I)\cdot v=v\}$ 和 $V^-=\{v\in V,(-I)\cdot v=-v\}$ 都是 V 的子表示, 且 $V=V^+\oplus V^-$. 由此推出 $-I$ 以 -1 作用于所缺的表示上.

---

[7] 所用到的方法可以让我们从 S_3 的特征标表构造 S_4 的特征标表: 将 S_4 作用于有 3 个元的 $(1,2)(3,4)$ 的共轭类, 这给出了一个群的满态射 $S_4\to S_3$, 并得到了 S_4 的表的前 3 列. 像在问题 3 的 (i) 那样, 可以证明还缺少 2 个维数为 3 的表示. 对应于 χ_1 的表示 V_1 由将平凡表示移到与 S_4 在 $\{1,2,3,4\}$ 上作用的置换表示上 (参看习题 1.9) 得到; 另一个则由对 V_1 用线性特征标符号差 ε 进行扭变得到.

(iii) 解释如何由此得到所缺失的 3 列的前 4 行 (关注 $\rho_V(g)$ 与 $\rho_V(-g)$ 之间的地方).

问题 4. 设 X 是一个缺失的 2 维表示.

(i) 证明 $\chi_X(C)=\pm i\sqrt{2}$(考虑 u,u^3,u^4 的特征值, 其中 $u=\rho_X(C)$).

(ii) 由此得到所缺失的两个 2 维表示间的关联, 并证明这两个之一 (以 V 记之, 另一个记为 V') 满足 $\chi_V(C)=i\sqrt{2}$.

(iii) 证明 $H=\{g\in G,\chi_V(g)=2\}$ 是 G 的一个正规子群; 由此推出 $\chi_V(T)\neq 2$(可以考虑 $STS^{-1}T$), 然后得到 $\chi_V(T)=-1$.

(iv) 解释如何完成 G 的特征标表.

问题 5. 计算与 G 在 $\mathbf{F}_3\times\mathbf{F}_3$ 上的作用相关联的置换表示 Y 的特征标和在 Y 的分解中不可约表示的重数.

[574] **问题 6.** 设 $B\subset G$ 是由上三角矩阵构成的子群, 而 $\eta:B\to\{\pm1\}$ 是一个线性特征标, 其定义为: 当 $d=1$ 时 $\eta\left(\begin{pmatrix}a&b\\0&d\end{pmatrix}\right)=1$, 而当 $d=-1$ 时 $\eta\left(\begin{pmatrix}a&b\\0&d\end{pmatrix}\right)=-1$.

(i) 计算 $|B|$.

(ii) 设 $W'=\mathrm{Ind}_B^G\eta$. 证明 $W'\cong W$ (计算 $\chi_{W'}(\pm I)$ 和 $\chi_{W'}(T)$ 的符号差).

问题 7. 计算在 $Z=W\otimes W\otimes W$ 的分解中的不可约表示的重数.

问题校正

问题 1. (i) (a) 如果 $v\neq0$ 而 $(v,g(v))$ 不是 K^2 的一组基, 那么 $g(v)$ 是 v 的一个倍数. 设 e_1,e_2 是 K^2 的标准基. 如果 $g(e_1)=\lambda_1e_1, g(e_2)=\lambda_2e_2$, 且若 g 不是位似变换, 于是 $\lambda_2\neq\lambda_1$, 从而 $g(e_1+e_2)$ 不是 e_1+e_2 的倍数; 由此推出 e_1,e_2,e_1+e_2 这三个向量中至少有一个使得 v 和 $g(v)$ 构成了 K^2 在 K 上的一组基.

(i) (b) 由于 g 不是位似变换, 故存在 $v\in K^2$ 使得 $(v,g(v))$ 是 K^2 的一组基. g 在这组基下的矩阵为 $\begin{pmatrix}0&a\\1&b\end{pmatrix}$, 因其迹为 b, 故 $b=\mathrm{Tr}(g)$, 而行列式为 $-a$, 故 $a=-\det(g)$. 于是 $g=P\begin{pmatrix}0&-\det(g)\\1&\mathrm{Tr}(g)\end{pmatrix}P^{-1}$, 其中 P 是列分别为 v 和 $g(v)$ 的矩阵. 得到结果.

(ii) 位似与所有元均交换, 因而它们的共轭类只有一个元. 由于在 G 中正好只有两个位似即 I 和 $-I$, 这已经给出了两个共轭类.

根据 (i), 其余的类双射地对应于 $(\det(g),\mathrm{Tr}(g))$ 的可能的值. 但因为 $\mathbf{F}_3^*$ 只有两个元并且 G 的元的行列式非零, 故 $\det(g)$ 可能取两个值 (即 1 和 -1), 而 $\mathrm{Tr}(g)$ 可能取 3 个值, 这给了我们 6 个类, 可以验证在 $g\mapsto(\det(g),\mathrm{Tr}(g))$ 下, $S,D,T,-T,C,-C$ 的像分别是 $(-1,0),(1,0),(1,-1),(1,-1),(-1,1),(-1,-1)$, 因此对于每个共轭类有

一个表示.

问题 2. (i) g 在 σ 的核中当且仅当所有向量在 g 作用下不变, 因而当且仅当对所有非零向量 v, $g(v)$ 与 v 共线. 按照问题 1 的 (i), 这蕴含了 g 是个位似变换. 由此推出 σ 的核是 $\{\pm I\}$. 由于 σ 的核的基数为 2, 那么它的像的基数为 $\frac{1}{2}|G| = 24 = |S_4|$, 这证明了 σ 为满射.

(ii) 注意, 因为 $-I$ 在 σ 的核中, 故 $\sigma(-g) = \sigma(g)$, 从而有

- $\sigma(I) = \sigma(-I) = \mathrm{id}$,
- $\sigma(S) = (1, 2)$,
- $\sigma(D) = (1, 2)(3, 4)$,
- $\sigma(T) = \sigma(-T) = (2, 3, 4)$,
- $\sigma(C) = \sigma(-C) = (1, 2, 3, 4)$.

(iii) 由于 $\sigma : G \to S_4$ 是一个满的群态射, 故映射 $\chi \mapsto \chi \circ \sigma$ 诱导了一个从 S_4 的特征标的集合到 G 的不可约特征标的集合的单射, 利用 S_4 的特征标表和 (ii), 它让我们可以填写出 G 的特征标表的前 5 列.

问题 3. (i) 由于不可约表示的个数与共轭类的个数相同, 故还缺少 $8 - 5 = 3$ 个表示. 如果以 d_1, d_2, d_3 记它们的维数, 那么 Burnside 公式 (推论 I.2.20) 表明 $d_1^2 + d_2^2 + d_3^2 + 1^2 + 1^2 + 2^2 + 3^2 + 3^2 = 48$, 从而 $d_1^2 + d_2^2 + d_3^2 = 24$. 这个方程只有一个解 (除了差一个置换外), 即 $d_1 = 4, d_2 = 2, d_3 = 2$.

(ii) 由于 $(-I)^2 = I$, 故有 $\rho_V(-I)^2 = 1$, 这表明 $\rho_V(-I)$ 是个对称态射, 因而对应于两个特征值 1 和 -1, V 是两个特征空间 V^+ 和 V^- 的直和. 另外, $-I$ 与 G 的所有元均交换, 故而当 v 是 $\rho_V(-I)$ 的对应于特征值 λ 的特征向量时, 有 $(-I) \cdot (g \cdot v) = g \cdot ((-I) \cdot v) = \lambda(g \cdot v)$; 由此得到 V^+ 和 V^- 在 G 的作用下稳定, 因而是 V 的一个子表示. [575]

现在, 如果 V 不可约, 则 $V = V^+$ 或 V^-, 但如果 $V = V^+$, 那么 σ 的核在 V 上的作用平凡, 这表明 V 是 S_4 的一个不可约表示; 因此它便不是缺失的那些表示的子表示, 这证明了 $-I$ 在缺失的表示上以 -1 作用.

(iii) 第一行由表示的维数构成, 因而为 $4, 2, 2$. 现在有 $\rho_V(-g) = \rho_V(-I)\rho_V(g) = -\rho_V(g)$, 因此 $\chi(-g) = -\chi_V(g)$. 由此, 且因为 S 和 D 的等价类在 $g \mapsto -g$ 不变及因为 $\mathrm{Tr}(-g) = -\mathrm{Tr}(g), \det(-g) = \det(g)$, 故得到第二行以及 $\chi_V(S)$ 和 $\chi_V(D)$ 为零.

问题 4. (i) 我们有 $C^3 = \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}, C_4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. 以 λ, μ 记 u 的特征值. 由于 $C^4 = -I$, 故 $u^4 = -1$ 从而 $\lambda^4 = \mu^4 = -1$. 现在, 因为 $\mathrm{Tr}(C^3) = 1 = \mathrm{Tr}(C), \det(C^3) = -1 = \det(C)$, 故 C^3 与 C 属于同一个共轭类. 如果 $g \in G$ 使得 $C^3 = gCg^{-1}$, 那么如果 $h = \rho_X(g)$, 则有 $u^3 = huh^{-1}$, 因此 u^3 和 u 具有相同的特征值. 由于这些特征值是 -1 的 4 次根, 故 $\{\lambda, \mu\} = \{e^{i\pi/4}, e^{3i\pi/4}\}$ 或者

$\{\lambda,\mu\}=\{-e^{i\pi/4},-e^{3i\pi/4}\}$, 从而 $\chi_C(X)=\mathrm{Tr}(u)=\pm(e^{i\pi/4}+e^{3i\pi/4})=\pm i\sqrt{2}$.

(ii) 表示 $X\otimes\varepsilon$ 是 G 的一个 2 维表示, 并由于 X 不可约而不可约, 又因为 $\chi_{X\otimes\varepsilon}(C)=\varepsilon(C)\chi_X(C)=-\chi_X(C)$ 而 $\chi_X(C)\neq 0$, 得知它不同于 X. 另外由于 $\varepsilon(-I)=1$, 这表明 $-I$ 在 $X\otimes\varepsilon$ 上以 -1 进行作用, 从而缺失的第二个 2 维表示是 $X\otimes\varepsilon$. 因为 $\{\chi_X(C),\chi_{X\otimes\varepsilon}(C)\}=\{i\sqrt{2},-i\sqrt{2}\}$, 故得到结论.

(iii) 如果 $g\in G$, 由于 $\chi_V(g)$ 是 $\rho_V(g)$ 的特征值的和, 于是等于两个单位根的和. 因此 $\chi_V(g)=2$ 当且仅当这两个特征值都等于 1, 又因为 $\rho_V(g)$ 是对角矩阵 (注记 I. 1.7), 从而当且仅当 $\rho_V(g)=1$. 换言之 H 是 ρ_V 的核; 它因此是 G 的一个正规子群.

如果 $T\in H$, 则同样地, $STS^{-1}T=\begin{pmatrix}1&1\\1&-1\end{pmatrix}$ 也属于 H, 而它却在 D 的共轭类中, 但 $\chi_V(D)=0$, 这引出了矛盾; 因此 $\chi_V(T)\neq 2$.

另外, $T^3=1$, 从而 $v=\rho_V(T)$ 的特征值是 3 次单位根. 又, $T^2=\begin{pmatrix}1&-1\\0&1\end{pmatrix}$ 在 T 的共轭类中, 因而 v^2 有 v 相同的特征值, 并且由于至少有一个特征值不同于 1, 这些特征值必是 $e^{2i\pi/3}$ 和 $e^{-2i\pi/3}$, 因此 $\chi_V(T)=\mathrm{Tr}(v)=e^{2i\pi/3}+e^{-2i\pi/3}=-1$.

(iv) 我们用关系式 $\chi_V(-g)=-\chi_V(g)$ 来完成第 7 列, 而用关系式 $\chi_{V'}(g)=\varepsilon(g)\chi_V(g)$ 来完成第 8 列. 最后, 为了完成第 6 列, 我们或者可以利用正则分解 (推论 I.2.20) 或者利用特征标表的列间的正交性 (注记 I.2.32), 因为在当下的情形下, 利用第一行时只允许一个符号差, 故它们导致了相同的结果.

问题 5. 由于 Y 是个置换表示故 $X_Y(g)$ 是 g 的不动点的个数, 也就是说 $3^{d(g)}$, 其中 $d(g)$ 是相伴于特征值 1 的特征空间的维数. 然而 1 是个特征值当且仅当 $X^2-\mathrm{Tr}(g)X+\det(g)$ 等于 $(X-1)^2$ 或 $(X-1)(X+1)$, 因此除了 $g=I$ 外 $d(g)=1$; 于是得到

$$\chi_Y(I)=9,\quad \chi_Y(-I)=1,\quad \chi_Y(S)=3,\quad \chi_Y(D)=1,$$
$$\chi_Y(T)=3,\quad \chi_Y(-T)=1,\quad \chi_Y(C)=1,\quad \chi_Y(-C)=1.$$

比较这些特征标, 因此得到 $Y\cong \mathbf{21}\oplus V_1\oplus W$. 如果不算是显然的话, 确实有许多方式来得到这个结果.

- 注意 G 在 $\mathbf{F}_3\times\mathbf{F}_3$ 上的作用有两条轨道, 即 $(0,0)$ 和另外一条, 即由 $e_{(0,0)}$ 生成的直线和由 $\sum_{(x,y)\neq(0,0)}e_{(x,y)}$ 生成的直线, 因此 Y 包含了两片平凡表示, 于是 Y 有形如 $Y\cong\mathbf{21}\oplus Y'$ 的分解. 由于 $\chi_{Y'}(I)=7,\chi_{Y'}(-I)=-1$ 且 $\chi_{Y'}(C)=\chi_{Y'}(-C)$, 我们推出 Y' 或者分解为 $W\oplus Y''$ 或者分解为 $V\oplus V'\oplus Y''$, 其中 Y'' 是个 3 维的表示, $-I$ 在其上的作用平凡. 因此我们有 $\chi_{Y''}(C)=-1,\chi_{Y''}(S)=1$, 那么剩下的仅有的可能性是 $Y''=V_1$. 注意到 $\chi_Y(T)$ 便可排除 $Y\cong V\oplus V'\oplus Y''$ 这个可能性. [576]
- 多少有点概念化的一个方法是将 Y 分解为形如 $Y^+\oplus Y^-$, 其中 Y^+ 和 Y^- 是对应于 $\rho_Y(-I)$ 的特征值 1 和 -1 的特征子空间. Y^+ 由对于 $x\in\mathbf{F}_3\times\mathbf{F}_3$ 的 $e_x+(-I)\cdot e_x$

生成, 它可分解为两个表示的直和, 其中一个是由 $e_{(0,0)}$ 生成的直线 Y_0, 另一个是由 f_i 生成的空间 Y_1, 其中 $f_i = \sum_{x\in\Delta_i} e_x$. Y_0 是个平凡表示, 而 Y_1 是由 G 在向量直线上作用诱导的置换表示 (它对应于 S_4 在 $\{1,2,3,4\}$ 上作用相伴的 S_4 的置换表示); 它的特征标是 $\mathbf{1}+\chi_1$, 由公式 $\chi_{Y^-} = \chi_Y - \chi_{Y^+}$ 可最终计算出 χ_{Y^-}. 用此方法可确定 Y 的同型分支, 这比计算不可约表示的重数来得更精确.

- 一个不那么人为的解决方法是利用计算重数的一般公式 (推论 I.2.15), 它要求计算共轭类的基数 (这可以通过 G 的共轭类与 S_4 的共轭类的关联做到) 从而计算出特征标的标量积.

问题 6. (i) 因为 $g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto (a,d,b)$ 诱导了一个由 B 到 $(\mathbf{F}_3^*)^2 \times \mathbf{F}_3$ 的双射, 故 $|B| = 12$.

(ii) 根据定理 I.3.11, 我们有 $\chi_{W'}(g) = \frac{1}{|B|}\sum_{s\in G, sgs^{-1}\in B} \eta(sgs^{-1})$. 现在,$|B| = 12$, 而前面对于 I 和 $-I$ 的公式, 以及 I 与 $-I$ 与所有元都交换, 从而属于 B, 于是给出了 $\chi_{W'}(I) = \frac{48}{12} = 4, \chi_{W'}(-I) = -4$; 因此 $W' \cong W$ 或者 $W' \cong Z \oplus Z'$, 其中 $\{Z, Z'\} \subset \{V, V'\}$.

另外, sTs^{-1} 仅有的特征值是 1, 从而, 如果 $sTs^{-1} \in B$, 则 $sTs^{-1} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, 故而 $\eta(sTs^{-1}) \geqslant 0$. 于是得到 $\chi_{W'}(T) \geqslant 0$; 使它成为可能只有 $W' \cong W$.

问题 7. 我们有 $\chi_Z(g) = \chi_W(g)^3$. 特别地, $\chi_Z(-I) = -\chi_Z(I)$, 故而 $-I$ 以 -1 作用在 Z 上, 因此 $Z \cong m_W W \oplus m_V V \oplus m_{V'} V'$, 从而 $\chi_Z = m_W\chi_W + m_V\chi_V + m_{V'}\chi'_V$. 将此恒等式在 C 上取值得到 $m_V = m_{V'}$, 而在 I 和 T 上取值则得到 $4m_W + 4m_V = 64$ 和 $m_W - 2m_V = 1$, 因此 $m_W = 11, m_V = 5$, 而 $Z \cong 11W \oplus 5V \oplus 5V'$.

H.4. $\mathbf{GL}_3(\mathbf{F}_2)$ 的特征标表

[577]

这个作业的目标是构造群 $G = \mathbf{GL}_3(\mathbf{F}_2)$ 的特征标表 (图 9), 其中的 $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ 是具有两个元的域 (在此域中我们有 $1 = -1, 2 = 0$).

	基数	特征多项式	极小多项式	阶
C_1	1	$(X-1)^3$	$X-1$	1
C_2	21	$(X-1)^3$	$(X-1)^2$	2
C_4	42	$(X-1)^3$	特征多项式	4
C_3	56	X^3-1	特征多项式	3
C_7	24	X^3+X+1	特征多项式	7
C'_7	24	X^3+X^2+1	特征多项式	7

	χ_1	χ_3	χ_3'	χ_6	χ_7	χ_8
C_1	1	3	3	6	7	8
C_2	1	-1	-1	2	-1	0
C_4	1	1	1	0	-1	0
C_3	1	0	0	0	1	-1
C_7	1	α	$\bar{\alpha}$	-1	0	1
C_7'	1	$\bar{\alpha}$	α	-1	0	1

图 9. $\mathbf{GL}_3(\mathbf{F}_2)$ 的共轭类表和特征标表

I. 共轭类

如果 K 是一个 (交换) 域, 且若 $A \in \mathbf{M}_n(K)$, 则以 $\mathrm{Car}(A)$ 记 A 的特征多项式, 而 $\mathrm{Min}(A)$ 记其极小多项式[(8)].

问题 0. 证明, 如果 p 是个素数, 则 $\mathbf{F}_p^n$ 在 $\mathbf{F}_p$ 上的一组基的个数是 $\prod_{i=0}^{n-1}(p^n - p^i)$. 由此推出 $|G| = 168$.

问题 1. 设 K 为域, $P = X^3 + a_2X^2 + a_1X + a_0 \in K[X]$, 而 X_P 是满足 $\mathrm{Car}(A) = \mathrm{Min}(A) = P$ 的 $A \in \mathbf{M}_3(K)$ 的集合.

(i) 证明, $A \in X_P$ 当且仅当 A 与 $\begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix}$ 共轭.

(ii) 设 $A \in X_P$. 证明 $\dim \mathrm{Ker}(A-1) = 0$ 或 1 依 $P(1) = 0$ 或 $P(1) \neq 1$ 而定.

(iii) 如果 $\mathrm{Car}(A) = (X-1)^3, \mathrm{Min}(A) = X - 1$, 那么 A 是什么? $\dim \mathrm{Ker}(A-1)$ 等于多少?

(iv) 证明, 当 $\mathrm{Car}(A) = (X-1)^3$ 而 $\mathrm{Min}(A) = (X-1)^2$ 时 $\dim \mathrm{Ker}(A-1) = 2$. 由此得到 A 共轭于 $\begin{pmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. (选取 $v \notin \mathrm{Ker}(A-1)$, 并找出 v, Av, A^2v 之间的关系.)

[(8)]我们要用到下面的一些结果.

- 多项式 $\mathrm{Car}(A)$ 和 $\mathrm{Min}(A)$ 在 $\mathbf{GL}_n(A)$ 中的元的共轭下不变 (即当 $P \in \mathbf{GL}_n(K)$ 时 $\mathrm{Car}(PAP^{-1}) = \mathrm{Car}(A)$ 及 $\mathrm{Min}(PAP^{-1}) = \mathrm{Min}(A)$).
- $\mathrm{Car}(A)$ 的次数等于 n, $\mathrm{Min}(A)$ 整除 $\mathrm{Car}(A)$ (Cayley-Hamilton 定理), 而 $\mathrm{Min}(A) = \mathrm{Car}(A)$ 当且仅当 $\mathrm{Car}(A)$ 在分解为不可约多项式时不包含指数 $\geqslant 2$ 的因子.
- 如果 $v \in K^n$, 使得 $P(A)\cdot v = 0$ 的 $P \in K[X]$ 的集合是一个包含 $\mathrm{Min}(A)$ 的理想, 并存在一个 $v \in K^n$, 使得 $\mathrm{Min}(A)$ 生成这个理想, 这时 $v, Av, \ldots, A^{d-1}v$ 是 K^n 的一个无关族, 其中 $d = \deg(\mathrm{Min}(A))$.

问题 2. 对于 $G=\mathbf{GL}_3(\mathbf{F}_2)$ 中的一个元 A, $\mathrm{Car}(A)$ 可能的值是些什么? 由此得到 G 的共轭类表并给出每个类的一个元.

问题 3. (i) 计算这些不同类的阶[9] (利用在 $\mathbf{F}_2[X]$ 中的因式分解) $X^2-1=(X-1)^2$, $X^4-1=(X-1)^4, X^8-X=X(X-1)(X^3+X+1)(X^3+X^2+1)$). [578]

(ii) 证明, 如果 $C\in\mathrm{Conj}(G)$, 而 $k\in\mathbf{Z}$, 则 $\{g^k, g\in C\}\in\mathrm{Conj}(G)$.

(iii) 证明 C_4 在 $g\mapsto g^3$ 下稳定, 而 C_3 在 $g\mapsto g^2$ 下稳定.

(iv) 证明 $g\mapsto g^2$ 将 C_4 映到 C_2 和 C_1, 而 C_2 映到 C_1.

(v) 证明 C_7 和 C_7' 在 $g\mapsto g^{-1}$ 下相互交替, 并在 $g\mapsto g^2$ 下稳定 (可利用在 $\mathbf{F}_2[X]$ 中的公式 $P(X)^2=P(X^2)$).

问题 4. (i) 证明 $N=\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}, a,b,c\in\mathbf{F}_2\right\}$ 是包含在 u 的中心化子中的 G 的一个子群, 其中 $u=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}$. 由此推出 $|C_2|$ 整除 21; 相等意味什么?

(ii) 证明如果 $C\in\mathrm{Conj}(G)$ 的阶为 n, 则 $|C|$ 整除 $|G|/n$. 等号在什么条件下成立?

(iii) 计算每个类的基数, 从而证明 C_3, C_4, C_7 或 C_7' 中的一个元 g 的中心化子是 G 的由 g 生成的子群, 而 C_2 的一个元的中心化子的基数等于 8.

II. 特征标表

问题 0. 设 $\omega=e^{2i\pi/7}, \alpha=\omega+\omega^2+\omega^4$. 计算 $\sum_{i=0}^{6}\omega^i$. 由此推出 $\alpha=\frac{-1+i\sqrt{7}}{2}$(可计算 α^2).

问题 1. 设 V 是 G 的一个表示. (我们将用到 I 中的问题 3.)

(i) 证明 $\chi_V(C_2)\in\mathbf{Z}$.

(ii) 证明 $\rho_V(C_4)$ 的算上重数的特征值在 $\lambda\mapsto\lambda^3$ 下稳定. 由此推出 $\chi_V(C_4)\in\mathbf{Z}$.

(iii) 同样地, 证明 $\chi_V(C_3)\in\mathbf{Z}$.

(iv) 证明存在整数 a,b,c 使得 $a+3b+3c=\dim V$ 以及 $\chi_V(C_7)=a+b\alpha+c\bar{\alpha}, \chi_V(C_7')=a+c\alpha+b\bar{\alpha}$.

问题 2. 表中的特征标 χ_1 是什么? 以 V_1 表示与其相伴的表示.

问题 3. 群 G 作用于向量空间 $\mathbf{F}_2^3$, 并且这个作用保持了 $\mathbf{F}_2^3$ 中的非零元的集合不变. 以 V_X 记其相伴的置换表示.

(i) 计算 V_X 的特征标. (利用 I 的问题 1.)

---

[9] 一个共轭类的阶是指它的任意元的阶.

(ii) 证明超平面 $V = \{\sum_{x\in X} \alpha_x e_x, \sum_{x\in X} \alpha_x = 0\}$ 在 G 下稳定, 并计算 V 的特征标 χ.

(iii) 由此推出 G 有一个 6 维的不可约表示 V_6(以 χ_6 表示其特征标); 它可以填写进这个表的哪一部分?

问题 4. 设 W 是 V_6 的二次交错积.

(i) 计算 $\chi_W, \langle\chi_W, \chi_W\rangle$ 和 $\langle\chi_W, \chi_6\rangle$. (利用 I 的问题 3.)

(ii) 方程 $131 = a^2 + b^2 + c^2 + d^2 (a \geqslant 8)$ 是什么? 推出除 V_1, V_6 外, 作为群 G 的不可约表示还有 8 维的 V_8, 7 维的 V_7, 3 维的 V_3 和 V_3' 以及 $W \cong V_7 \oplus V_8$(以 [579] $\chi_8, \chi_7, \chi_3, \chi_3'$ 分别代表这些表示的特征标). 它们可填写进此表的哪一部分?

问题 5. (i) 证明, 如果 χ 是 G 的一个表示的特征标, 则 $\overline{\chi}$ 也是 G 的一个表示的特征标. 由此推出 $\mathrm{Irr}(G)$ 在 $\chi \to \overline{\chi}$ 下不变.

(ii) 证明 χ_7 是实的.

(iii) 证明 $|\chi_7(C_7)| < \sqrt{168/24}$. 由此推出 $\chi_7(C_7) = \chi_7(C_7') = 0$.

(iv) $\langle\chi_7, \chi_1\rangle, \langle\chi_7, \chi_6\rangle$ 和 $\langle\chi_7, \chi_7\rangle$ 等于多少? 由此推出 χ_7, 然后推出 χ_8.

问题 6. (i) 设 V 是 G 的一个 3 维表示. 证明, 如果 $\chi_V(C_7)$ 是实的, 则 $\chi_V(C_7) = \chi_V(C_7') = 3$. 由此推出 V 不是不可约的.

(ii) 证明 $\chi_3' = \overline{\chi_3}$, 并解释如何完成此特征标表.

问题 7. G 以共轭作用于 C_7; 设 Y 是其相伴的置换表示.

(i) 利用 I 的问题 4(iii) 证明, $g \neq 1$ 在 $h \in C_7$ 的中心化子中当且仅当 h 是 g 的一个幂.

(ii) 计算 χ_Y 并由此推出 $Y \cong V_1 \oplus V_7 \oplus 2V_8$.

(iii) 构造 Y 的子表示 W_1, W_7, W_8, W_8' 使得 $Y = W_1 \oplus W_7 \oplus W_8 \oplus W_8'$. (我们可以考虑 $f_{g,\beta} = e_g + \beta e_{g^2} + \beta^2 e_{g^4}$, 其中 $g \in C_7, \beta \in \{1, j, j^2\}$, 而 $j = e^{2i\pi/3}$.)

问题 8. 由这个特征标表, 证明 G 是单的[10]. (如果 G 不是单的, 那么考虑从 G 的一个商的某个不可约表示着手去得到 G 的一个表示.)

问题校正

I. 共轭类

问题 0. 如果 K 为域, K^n 在 K 上的一组基由第一个为非零的向量 e_1, 第二个不在 e_1 生成的直线上的向量 e_2, 而第三个不在 e_1 和 e_2 生成的平面上的 e_3 等构成. 如果 $|K| = q$, 故 e_1 有 $q^n - 1$ 个不同的选择, e_2 有 $q^n - q$ 个选择, e_3 有 $q^n - q^2$ 个选择, 等等, 总起来有 $(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})$ 组不同的基.

[10]这是在 A_5 (基数为 60) 后最小的非交换单群; 它也同构于 $\mathbf{PSL}_2(\mathbf{F}_7) = \mathbf{SL}_2(\mathbf{F}_7)/\{\pm 1\}$, 但要构造出这个同构颇费工夫.

现在, 将矩阵 $A \in \mathbf{GL}_n(K)$ 映成它的 n 个列向量是从 $\mathbf{GL}_n(K)$ 到 K^n 的所有基族的集合上的一个双射; $\mathbf{GL}_n(K)$ 的基数因而等于 $\prod_{i=0}^{n-1}(q^n - q^i)$. 在我们现在感兴趣的情形中, $n = 3, q = 2$, 故有 $|G| = (8-1)(8-2)(8-4) = 168$.

问题 1. (i) 由于 $\mathrm{Min}(A)$ 是 3 次的, 故存在 v 使得 v, Av, A^2v 构成 K^3 的一组基. 另外, $\mathrm{Min}(A) \cdot v = 0$. 从而 $A \cdot (A^2v) = -a_2A^2v - a_1Av - a_0v$. 因此, 如果 $U \in \mathbf{GL}_3(K)$ 是其列为 v, Av, A^2v 的矩阵时, 则得到 $U^{-1}AU = B$, 其中 $B = \begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix}$.

反之, 如果 A 共轭于 B, 则 $\mathrm{Car}(A) = \mathrm{Car}(B)$ 以及 $\mathrm{Min}(A) = \mathrm{Min}(B)$. 现在, 按最后一列展开 $\begin{vmatrix} X & 0 & a_0 \\ -1 & X & a_1 \\ 0 & -1 & X + a_2 \end{vmatrix}$, 得到了 $\mathrm{Car}(B) = (X+a_2)X^2 - a_1(-X) + a_0 = P$. 最后, 如果记 K^3 的标准基为 e_1, e_2, e_3, 则有 $Be_1 = e_2$ 和 $B^2e_1 = e_3$, 于是 e_1, Be_1, B^2e_1 构成一个无关族, 从而有一个次数 $\geqslant 3$ 的非零多项式 Q 使得 $Q(B) \cdot e_1 = 0$. 因此得到 $\mathrm{Min}(B)$ 的次数 $\geqslant 3$, 并由于它整除 $\mathrm{Car}(B)$, 我们有 $\mathrm{Min}(B) = \mathrm{Car}(B) = P$, 即为所求. [580]

(ii) 设 v 是使得 v, Av, A^2v 为 K^3 的一组基的向量. 由于 $A^3v = -a_0v - a_1Av - a_2A^2v$, 故得到 $(A-1)(x_0v + x_1Av + x_2A^2v) = (-a_0x_2 - x_0)v + (x_0 - a_1x_2 - x_1)Av + (x_1 - a_2x_2 - x_2)A^2v$. 由此得知 $\mathrm{Ker}(A-1)$ 是那些满足 $x_0 = -a_0x_2, x_1 = -(a_0+a_1)x_2$ 和 $x_2(a_2 + a_0 + a_1 + 1) = 0$ 的集合, 但由于 $a_0 + a_1 + a_2 + 1 = P(1)$, 于是可看出, 如果 $P(1) \neq 0$, 则此空间的维数为 0, 而如果 $P(1) = 0$, 则维数为 1.

(iii) 如果 $\mathrm{Min}(A) = X - 1$, 则 $A = 1$, 因此 $\mathrm{Ker}(A-1)$ 的维数为 3.

(iv) 如果 $(A-1)^2 = 0$, 则有 $\mathrm{Im}(A-1) \subset \mathrm{Ker}(A-1)$, 又由于 $\dim(\mathrm{Im}(A-1)) + \dim(\mathrm{Ker}(A-1)) = 3$, 这表明 $\dim(\mathrm{Ker}(A-1)) \geqslant 2$. 由此, 并因为 $A \neq 1$, 便推出 $\mathrm{Ker}(A-1)$ 的维数为 2, 从而 $\dim(\mathrm{Ker}(A-1)) < 3$.

如果 $v \notin \mathrm{Ker}(A-1)$, 由于 1 是仅有的特征值, 故 v, Av 是一个无关族. 特别地, 由 v 和 Av 生成的平面不等于 $\mathrm{Ker}(A-1)$, 那么可以用一个 $w \in \mathrm{Ker}(A-1)$ 补充进 v 和 Av 得到 K^3 的一组基. 另外, 我们有 $(A-1)^2v = 0$, 因此 $A \cdot (Av) = -v + 2Av$. 因此知, 如果以 $U \in \mathbf{GL}_3(K)$ 记其列为 v, Av 和 w 的矩阵, 则有 $U^{-1}AU = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, 得证.

问题 2. 由于特征多项式的常数项是此行列式, 那么它不为零当且仅当其矩阵可逆. 因此对于 G 的一个元有 4 个可能的特征多项式, 即 $X^3 + 1 = X^3 - 1 = (X-1)(X^2 + X + 1), X^3 + X + 1, X^3 + X^2 + 1$ 和 $X^3 + X^2 + X + 1 = (X-1)^3$.

- 如果 $\mathrm{Car}(A) = X^3 + 1 = X^3 - 1$, 则有 $\mathrm{Min}(A) = X^3 + 1$: 因为 $X^3 + 1$ 没有重因

子, 从而根据问题 1 的 (i), A 共轭于 $\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$.

- 同样地, 如果 $\mathrm{Car}(A)=X^3+X+1$, 则 A 共轭于 $\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix}$.
- 同样地, 如果 $\mathrm{Car}(A)=X^3+X+1$, 则 A 共轭于 $\begin{pmatrix}0&0&1\\1&0&0\\0&1&1\end{pmatrix}$.
- 如果 $\mathrm{Car}(A)=(X-1)^3$, 那么 $\mathrm{Min}(A)$ 有三种可能.

　— 如果 $\mathrm{Min}(A)=(X-1)$, 则 $A=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$.

　— 如果 $\mathrm{Min}(A)=(X-1)^2$, 则根据问题 1 的 (iii), A 共轭于 $\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}$.

　— 如果 $\mathrm{Min}(A)=(X-1)^3$, 则根据问题 1 的 (i), A 共轭于 $\begin{pmatrix}0&0&1\\1&0&1\\0&1&1\end{pmatrix}$.

由于 $\mathrm{Car}(A)$ 和 $\mathrm{Min}(A)$ 在共轭下不变, 故前面的讨论表明这些共轭类与可能的所有偶对 $(\mathrm{Car}(A),\mathrm{Min}(A))$ 之间有一个双射. 因此我们得到表中的类 C_1,C_2,C_4,C_3,C_7,C_7' 分别由以下矩阵代表:

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix},\begin{pmatrix}0&0&1\\1&0&1\\0&1&1\end{pmatrix},\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix},\begin{pmatrix}0&0&1\\1&0&1\\0&1&0\end{pmatrix},\begin{pmatrix}0&0&1\\1&0&0\\0&1&1\end{pmatrix}.$$

问题 3. (i) • C_1 可化为阶为 1 的中性元.

- 由于在 $\mathbf{F}_2[X]$ 中 $(X-1)^2=X^2-1$, 故 C_2 中一个元的阶因而整除 2, 并由于不可能为 1, 故为 2.
- 由于 $(X-1)^3$ 在 $\mathbf{F}_2[X]$ 中整除 X^4-1, 故 C_4 中的元 A 整除 4, 并由于 A 的极小多项式是 $(X-1)^3$, 从而 $A^2-1\neq 0$, 故 A 的阶为 4.
- 由于 C_3 中的元被 X^3-1 化零, 故其阶整除 3, 从而阶为 3.
- 由于 X^3+X+1 和 X^3+X^2+1 在 $\mathbf{F}_2[X]$ 中整除 X^7-1, C_7 和 C_7' 中的元的阶整除 7, 从而等于 7.

(ii) 设 $g_0\in C$. 于是 $C=\{hg_0h^{-1},h\in G\}$, 并由于 $(hg_0h^{-1})^k=hg_0^kh^{-1}$, 由此推出 $\{g^k,g\in C\}$ 是 g_0^k 的共轭类.

(iii) 如果 g 的阶为 4, 则 g^3 的阶也为 4. 于是 $g \mapsto g^3$ 将 C_4 映到阶为 4 的元构成的共轭类, 并且由于已经有了一个这样的类, 即 C_4, 故证明了 $g \mapsto g^3$ 使 C_4 稳定. 由同样的理由, 对于唯一的由 3 阶元构成的 C_3, 它在 $g \mapsto g^2$ 下稳定. [581]

(iv) 结果来自: 当 g 的阶为 4 时, g^2 的阶为 2, 而 g 的阶为 1 或 2 时其阶为 1, 并且只存在唯一的阶为 1 或 2 的类.

(v) 如果 $A \in \mathbf{GL}_n(K)$, 而 $\mathrm{Car}(A) = P$, 则 A^{-1} 的特征多项式因而有 $\mathrm{Car}(A^{-1}) = \det(A^{-1} - X) = (\det A^{-1})X^n \det(X^{-1} - A) = (\det A)^{-1}X^n P(X^{-1})$. 这个公式表明, 当 g 的特征多项式为 $X^3 + X^2 + 1$ 时, g^{-1} 的特征多项式为 $X^3 + X + 1$, 反之亦然. 因此, C_7 和 C_7' 在 $g \mapsto g^{-1}$ 下交换.

如果 $P(A) = 0$, 则 $P(A)^2 = 0$, 并由于是在 $\mathbf{F}_2$ 上, 故 $P(A)^2 = P(A^2)$, 这证明了 A^2 的极小多项式整除 A 的特征多项式. 在 C_7 和 C_7' 的情形, 这些特征多项式是不可约的, 那么这个整除性表明它们相等, 这便证明了 C_7 和 C_7' 在 $g \mapsto g^2$ 下稳定.

问题 4. (i) $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}$. 此公式明显表明 N 在乘积下稳定, 因而是有限群 G 的一个子群并且 N 的每个元都与 u 交换.

现在, 因为 C_2 包含了所有 2 阶的元, 故 C_2 是 u 的类. 因此 $|C_2| = |G|/|Z_u|$, 其中 Z_u 为 u 的中心化子. 然而 Z_u 包含了 N, 从而 $|Z_u|$ 是 $|N| = 8$ 的倍数. 于是 $|C_2|$ 整除 $|G|/8 = 21$, 而等式成立当且仅当 $|Z_u| = 8$.

(ii) 设 $g \in C$. 如果 C 的阶等于 n, 则由 g 生成的这个子群的基数为 n. 由于它包含在 g 的中心化子 Z_g 中, 故而 $n \mid |Z_g|$, 又由于 $|C| = |G|/|Z_g|$, 则得知 $|C|$ 整除 $|G|/n$, 而等式成立当且仅当 Z_g 由 g 生成.

(iii) 我们有 $|C_1| = 1$, 从 (i) 和 (ii) 可清楚看出 $|C_2|$ 整除 21, $|C_4|$ 整除 $168/4 = 42$, $|C_3|$ 整除 $168/3 = 56$ 以及 $|C_7|$ 和 $|C_7'|$ 整除 $168/7 = 24$. 由于 $168 = |G| = |C_1| + |C_2| + |C_4| + |C_3| + |C_7| + |C_7'|$, 且由于 $1 + 21 + 42 + 56 + 24 + 24 = 168$, 故上面的整除关系是个相等关系, 因而得到结论.

II. 特征标表

问题 0. 我们有 $\sum_{i=0}^{6} \omega^i = \frac{\omega^7 - 1}{\omega - 1} = 0$. 由此得到

$$\alpha^2 = \omega^2 + \omega^4 + \omega + 2\omega^3 + 2\omega^5 + 2\omega^7 = -2 - \alpha.$$

故有 $\alpha = \frac{-1 \pm i\sqrt{7}}{2}$, 且由于 $\mathrm{Im}(\alpha) = \sin\frac{2\pi}{7} + \sin\frac{4\pi}{7} - \sin\frac{\pi}{7} > 0$, 即为所求.

问题 1. (i) $\chi_V(g)$ 是 $\rho_V(g)$ 的特征值计入重数的和, 并由于当 $g \in C_2$ 时 $\rho_V(g)^2 = \rho_V(g^2) = 1$, 这些特征值是 ± 1, 因而是整数, 故得结论.

(ii) 设 $g \in C_4$. 从 I 的问题 3(iii) 得到 $g^3 \in C_4$, 从而存在 $h \in G$ 使得 $g^3 = hgh^{-1}$. 于是有 $\rho_V(g)^3 = \rho_V(g^3) = \rho_V(hgh^{-1}) = u\rho_V(g)u^{-1}$, 其中 $u = \rho_V(h)$. 故得知 $\rho_V(g)^3$

与 $\rho_V(g)$ 共轭, 因而有相同重数的相同特征值. 因为 $\rho_V(g)^3$ 的特征值由 $\rho_V(g)$ 的特征值的立方得到, 这便证明了 $\rho_V(g)$ 的计入重数的特征值在 $\lambda \mapsto \lambda^3$ 下稳定.

现在, 由于 g 的阶为 4, 故 $\rho_V(g)$ 的特征值属于 $\{1, -1, i, -i\}$. 以 a, b, c, d 分别记它们的重数. 因为 $i^3 = -i$, 于是由前述知 $c = d$, 因而 $\chi_V(g) = a+b(-1)+ci+d(-i) = a - b \in \mathbf{Z}$, 为所要证明的.

(iii) $\rho_V(g)$ 属于 $\{1, j, j^2\}$, 其中 $j = e^{2i\pi/3}$, 并根据 I 的问题 3(iii), g 共轭于 g^2, 像上面那样, 得知 j 和 j^2 的重数相同, 但 $j + j^2 = -1 \in \mathbf{Z}$, 故得结论.

[582] (iv) 设 $g \in C_7$. 由于 g 的阶为 7, 故 $\rho_V(g)$ 的特征值属于 $\{\omega^i, 0 \leqslant i \leqslant 6\}$. 再者, 由于 C_7 在 $g \mapsto g^2$ 下稳定, 于是 ω 的重数与 ω^2 和 ω^4 的重数相同, 而 $\omega^{-1} = \omega^6$ 的重数与 $\omega^{-2} = \omega^5$ 和 $\omega^{-4} = \omega^3$ 的重数相同, 因而有 $a + 3b + 3c = \dim V$ 和 $\chi_V(C_7) = \chi_V(g) = a + b(\omega + \omega^2 + \omega^4) + c(\omega^{-1} + \omega^{-2} + \omega^{-4}) = a + b\alpha + c\bar{\alpha}$. 最后, 由于 $g^{-1} \in C_7'$, 且由于 $\rho_V(g^{-1})$ 的特征值是 $\rho_V(g)$ 的特征值的逆, 故得到 $\chi_V(C_7') = \chi_V(g^{-1}) = a + b\bar{\alpha} + c\alpha$.

问题 2. χ_1 是平凡表示的特征标.

问题 3. (i) 由于 V_X 是个置换表示, $\chi_{V_X}(g)$ 便是 g 的不动点的个数, 又由于 g 的不动点是除原点以外的特征值 1 相伴的特征空间, 故如果此特征空间为零, 则 $\chi_{V_X}(g) = 0$, 而如果其维数为 1, 则 $\chi_{V_X}(g) = 1$, 当维数为 2 时, $\chi_{V_X}(g) = 3$, 当维数为 3 时, $\chi_{V_X}(g) = 7$, 因此有:

- 因为 1 不是特征多项式的根, 故 $\chi_{V_X}(C_7) = \chi_{V_X}(C_7') = 0$.
- 根据 I 的问题 2(ii), $\chi_{V_X}(C_3) = 1$.
- 根据 I 的问题 2 的 (iii),(iv) 和 (ii) 有 $\chi_{V_X}(C_1) = 7, \chi_{V_X}(C_2) = 3$ 和 $\chi_{V_X}(C_4) = 1$.

(ii) $g \cdot \sum_{x\in X} \alpha_x e_x = \sum_{x\in X} \alpha_x e_{g\cdot x} = \sum_{x\in X} \alpha_{g^{-1}\cdot x} e_x$, 并由于 $x \mapsto g^{-1}\cdot x$ 是 X 的一个双射, 故有 $\sum_{x\in X} \alpha_{g^{-1}\cdot x} = \sum_{x\in X} \alpha_x$. 由此推出超平面 $V = \{\sum_{x\in X} \alpha_x e_x, \sum_{x\in X} \alpha_x\}$ 的稳定性.

由 $\sum_{x\in X} e_x$ 生成的直线 Δ 在 G 下不动, 因而给出了 V_X 的一个子表示, 其特征标为 χ_1. 由于 $V_X = \Delta \oplus V$, 故 $\chi_V = \chi_{V_X} - \chi_1$, 这给出了 $\chi_V(C_1) = 6, \chi_V(C_2) = 3, \chi_V(C_4) = 0, \chi_V(C_3) = 0, \chi_V(C_7) = \chi_V(C_7') = -1$.

(iii) $\langle \chi_V, \chi_V \rangle = \frac{1}{168}(6^2 + 21\cdot 2^2 + 42\cdot 0^2 + 56\cdot 0^2 + 24\cdot(-1)^2 + 24\cdot(-1)^2) = 1$, 这证明了 V 是个不可约表示, 并由于 $\chi_V(C_1) = 6$, 故其维数为 6. 这让我们可以填写对应于表中 χ_6 的那一列.

问题 4. (i) 我们有 $\chi_W(g) = \frac{1}{2}(\chi_6(g)^2 - \chi_6(g^2))$. 利用 I 的问题 3 的 (iii),(iv) 和 (v), 由此得到

$$\chi_W(C_1) = \frac{1}{2}(\chi_6(C_1)^2 - \chi_6(C_1)) = 15, \quad \chi_W(C_2) = \frac{1}{2}(\chi_6(C_2)^2 - \chi_6(C_1)) = -1,$$
$$\chi_W(C_4) = \frac{1}{2}(\chi_6(C_4)^2 - \chi_6(C_2)) = -1, \quad \chi_W(C_3) = \frac{1}{2}(\chi_6(C_3)^2 - \chi_6(C_3)) = 0,$$

$$\chi_W(C_7) = \frac{1}{2}(\chi_6(C_7)^2 - \chi_6(C_7)) = 1, \quad \chi_W(C_7') = \frac{1}{2}(\chi_6(C_7')^2 - \chi_6(C_7')) = 1.$$

由此得到 $\langle \chi_W, \chi_W \rangle = \frac{1}{168}(15^2+21\cdot(-1)^2+42\cdot(-1)^2+56\cdot 0^2+24\cdot 1^2+24\cdot 1^2) = 2$, 同样 $\langle \chi_W, \chi_6 \rangle = \frac{1}{168}(15\cdot 6+21\cdot(-1)\cdot 2+42\cdot(-1)\cdot 0+56\cdot 0^2+24\cdot 1\cdot(-1)+24\cdot 1\cdot(-1)) = 0$.

(ii) 由上一个问题得知 W 是两个维数之和为 15 的不可约表示的和, 且它们不同构于 V_6; 特别地, G 有一个维数 $\geqslant 8$ 的不可约表示.

另外, 由于 G 有 6 个共轭类, 故它有不同于 V_1 和 V_6 的另外 4 个不可约表示. 如果 a, b, c, d 分别是它们的维数, 则由 Burnside 公式有 $a^2+b^2+c^2+d^2 = 168-1^2-6^2 = 131$. 对于 $a \geqslant 8$ 的这个方程仅有的解为 $131 = 9^2+5^2+4^2+3^2$ 和 $131 = 8^2+7^2+3^2+3^2$.

第一个解可以排除, 原因是, 如果这样则要使 W 为 V_6 和一个 9 维表示的和, 但 V_6 不是 W 的一个不可约分支. 因此只有第二种情形. 证完.

问题 5. (i) 设 χ 为 G 的一个表示的特征标, 而 $\rho: G \to \mathbf{GL}_n(\mathbf{C})$ 是伴随 χ 的表示的群态射. 于是取 $\rho(g)$ 的系数的共轭定义的 $\bar{\rho}$ 也是一个群态射, 因为 $\mathrm{Tr}(\bar{\rho}(g)) = \overline{\mathrm{Tr}(\rho(g))}$, 故与其相伴的表示的特征标便为 $\bar{\chi}$(也可以取对偶表示). 现在, 我们有 $\langle \bar{\chi}, \bar{\chi} \rangle = \langle \chi, \chi \rangle$, [583] 因此 $\langle \bar{\chi}, \bar{\chi} \rangle = 1$ 当且仅当 $\langle \chi, \chi \rangle = 1$, 这证明了 $\bar{\chi} \in \mathrm{Irr}(G)$ 当且仅当 $\chi \in \mathrm{Irr}(G)$. 得证.

(ii) 也一直有唯一的 7 维表示, 故 $\bar{\chi}_7 = \chi_7$.

(iii) 我们有 $1 = \langle \bar{\chi}_7, \bar{\chi}_7 \rangle > \frac{24}{168}|\chi_7(C_7)|^2$, 因而 $|\chi_7(C_7)| < \sqrt{168/24} < 7$. 另外 (问题 I(iv)), 存在整数 a, b, c 使得 $a+3b+3c = 7$ 以及 $a+b\alpha+c\bar{\alpha} = \chi_7(C_7)$. 由于 $\chi_7(C_7) \in \mathbf{R}$, 这表明 $b = c$. 因此我们有两种可能: 要么 $a = 7, b = c = 0$ 从而 $\chi_7(C_7) = 7$, 这与不等式 $|\chi_7(C_7)| < 7$ 矛盾, 要么 $a = b = c = 1$, 从而 $\chi_7(C_7') = \chi_7(C_7) = 1+\alpha+\bar{\alpha} = \sum_{i=0}^{6} \omega^i = 0$.

(iv) 特征标的法正交性蕴含了 $\langle \chi_7, \chi_1 \rangle = 0, \langle \chi_7, \chi_6 \rangle = 0$ 和 $\langle \chi_7, \chi_7 \rangle = 1$. 令 $a = \chi_7(C_2), b = \chi_7(C_4), c = \chi_7(C_3)$, 并利用 $\chi_7(C_1) = \dim V_7 = 7$, 我们便得到 $7+21a+42b+56c = 0, 42+21\cdot 2a = 0$ 和 $7^2+21a^2+42b^2+56c^2 = 168$. 因此, $a = -1, 3b+4c = 1$ 和 $3b^2+4b^2 = 7$. 由于 b 和 c 是整数, 这些关系给出了 $b = -1, c = 1$. 这便添进到 χ_7 的列中.

由公式 $\chi_8 = \chi_W - \chi_7$ 便确定出 χ_8.

问题 6. (i) 根据问题 1(iv), 存在满足 $a+3b+3c = 3$ 和 $a+b\alpha+c\bar{\alpha} = \chi_V(C_7)$ 的整数 a, b, c. 如果 $\chi_V(C_7)$ 是实数, 则有 $b = c$, 这表明 $b = c = 0$, 从而 $a = 3$. 于是我们有 $\chi_V(C_7') = a+b\bar{\alpha}+c\alpha = 3$. 由此得到 $\langle \chi_V, \chi_V \rangle \geqslant \frac{1}{168}(24\cdot 3^2+24\cdot 3^2) > 1$, 它证明了 V 不是不可约的.

(ii) 从前面的命题得知 χ_3 不是实数, 因此 $\bar{\chi}_3 \neq \chi_3$. 由于 G 中仅有的另一个 3 次特征标是 χ_3', 因此 $\chi_3' = \bar{\chi}_3$. 又由于 $\chi_3(C_7)$ 非实数, 故有 $\chi_3(C_7) \in \{\alpha, \bar{\alpha}\}$, 必要时可将 χ_3 换作它的共轭, 故不妨设 $\chi_3(C_7) = \alpha$. 因此有 $\chi_3(C_7') = \bar{\alpha}, \chi_3'(C_7) = \bar{\alpha}$ 和 $\chi_3'(C_7') = \alpha$.

除此以外, $\chi_3(C_1), \chi_3(C_2), \chi_3(C_4), \chi_3(C_3)$ 都是实的. 我们有 $\chi_3(C_1) = \chi_3'(C_1)$,

$\chi_3(C_2)=\chi_3'(C_2), \chi_3(C_4)=\chi_3'(C_4), \chi_3(C_3)=\chi_3'(C_3)$. 利用 $\chi_1+3\chi_3+3\chi_3'+6\chi_6+7\chi_7+8\chi_8$ 是正则特征标这个事实便完成了特征标表的填写.

问题 7. (i) 根据 I 的问题 4(v), h 的中心化子是由 h 生成的子群, 它同构于 $\mathbf{Z}/7\mathbf{Z}$. 由此推出这个中心化子的每个元 $g\neq 1$ 都是一个生成元, 因此, 如果 $g\neq 1$ 在 h 的中心化子中, 则 h 是 g 的一个幂. 反方向的断言则是显见的, 故得结论.

(ii) 由于 Y 是一个置换表示, 故 $\chi_Y(g)$ 是 g 的不动点的个数. 但 $ghg^{-1}=h$ 当且仅当 g 在 h 的中心化子中.

如果 $g=1$, 上面条件总成立, 故 $\chi_Y(C_1)=|C_7|=24$.

如果 $g\neq 1$, 由 (i) 知, 满足此条件当且仅当 h 是 g 的一个幂. 换句话说, 这导致了去计算属于 C_7 的 g 的幂的个数, 因此给出了:

- 因为一个 2,3,4 阶的元不可能是一个 7 阶元的幂, 故 $\chi_Y(C_2)=\chi_Y(C_4)=\chi_Y(C_3)=0$.
- $\chi_Y(C_7)=3$(如果 $g\in C_7$, 则 $g,g^2,g^4\in C_7$) 而 $\chi_Y(C_7')=3$(如果 $g\in C_7'$, 则 $g^{-1},g^{-2},g^{-4}\in C_7$).

我们有 $\chi_Y=\chi_1+\chi_7+2\chi_8$, 这证明了 Y 同构于 $V_1\oplus V_7\oplus 2V_8$.

(iii) 向量 $f_{x,\beta}, f_{x^2,\beta}$ 和 $f_{x^4,\beta}$ 共线, 并有 $g\cdot f_{x,\beta}=f_{gxg^{-1},\beta}$. 由此得知由 $\{f_{x,\beta}, x\in C_7\}$ 生成的 Y_β 是一个在 G 下稳定的维数 $\leqslant 8$ 的空间. 又, 由 $f_{x,\beta}, f_{x^2,\beta}, f_{x^4,\beta}$ 生成的空间与由 e_x, e_{x^2}, e_{x^4} 生成的空间相同. 由此得到 $Y=Y_1+Y_j+Y_{j^2}$, 故由于维数的缘故有 $Y=Y_1\oplus Y_j\oplus Y_{j^2}$.

现在, Y_1 可分解为由 $\sum_{x\in C_7} e_x$ 生成的直线 W_1 和 W_7 的直和, 后者是 Y_1 与超平面 $\{\sum_{x\in C_7}\alpha_x e_x, \sum_{x\in C_7}\alpha_x=0\}$ 的交 (按常用的推理知其在 G 下稳定). 令 [584] $Y_j=W_8, Y_{j^2}=W_8'$ 便给出了所要的 Y 的分解.

问题 8. 设 H 是 G 的一个不等于 G 的正规子群. 如果以 G' 记商 G/H, 且 V 为 G' 的一个非平凡不可约表示, 则 V 也可以让 $g\in G$ 通过它在 G' 中的像的作用看成是 G 的一个表示. 由于对于每个 $v\neq 0$, $\{g\cdot v, g\in G\}$ 也是 $\{g'\cdot v, g'\in G'\}$, 而这个集合生成了 V, 故这个表示是不可约的. 特征标 χ_V 在 H 上取值 $\dim(V)=\chi_V(C_1)$. 然而 $\mathrm{Irr}(G)$ 中的唯一使得存在 $C\neq C_1$ 有 $\chi(C)=\chi(C_1)$ 的元 χ 是 χ_1. 由此得到 $H=1$, 从而 G 为单的.

[585] H.5. 连续函数的傅里叶系数

本节的目的是证明 $L^1(\mathbf{R}/\mathbf{Z})$ 中函数的傅里叶系数趋向 0 (是黎曼 – 勒贝格定理的离散形式), 但一个趋向 0 的序列不必是 $L^1(\mathbf{R}/\mathbf{Z})$ 中的一个元的傅里叶系数的序列.

部分 1. 以 E 记具有范数 $\|\ \|_\infty$ 的空间 $\mathscr{C}(\mathbf{R}/\mathbf{Z})$, 而 $F=L^1(\mathbf{R}/\mathbf{Z})$ 记 E 在 $\|\ \|_1$ 下的完备化, 其中范数 $\|\ \|_1$ 的定义是 $\|f\|_1=\int_0^1|f(x)|dx$. 最后, 令 E^* 为 E 的对偶, 并

赋予对偶范数 $\| \|_{E^*}$.

(i) 如果 $f, g \in E$, 令 $\Lambda_f(g) = \int_0^1 f(x)g(x)dx$. 证明 $g \mapsto \Lambda_f(g)$ 定义了 E^* 中的一个元, 而 $f \mapsto \Lambda_f$ 是从 E 到 E^* 的线性连续映射, 这里的连续性是指相对于范数 $\| \|_1$ 的.

(ii) 由此推出 $f \mapsto \Lambda_f$ 可以以唯一的方式延拓为从 F 到 E^* 的连续线性映射.

(iii) 如果 $n \in \mathbf{N} - \{0\}$, 令 $\phi_n : \mathbf{R} \to [-1, 1]$ 为一个定义在 $x \geqslant 0$ 上的连续的奇函数: 当 $x \leqslant 1/2n$ 时 $\phi_n(x) = 0$, 而当 $1/2n \leqslant x \leqslant 1/n$ 时 $\phi_n(x) = 2nx - 1$, 当 $x \geqslant 1/n$ 时 $\phi_n(x) = 1$. 令 $f \in E - \{0\}$, 并定义 g_n 为: 当 $f(x) \neq 0$ 时 $g_n(x) = \frac{\overline{f(x)}}{|f(x)|}\phi_n(|f(x)|)$, 而当 $f(x) = 0$ 时 $g_n(x) = 0$. 证明 $g_n \in E$, 并且当 n 充分大时 $\|g_n\|_\infty = 1$.

(iv) 设 $h_n = |f| - g_n f$. 证明 $\|h_n(x)\|_\infty \leqslant \frac{1}{n}$. 由此推出 $\|\Lambda_f\|_{E^*} = \|f\|_1$.

(v) 证明 $f \mapsto \Lambda_f$ 是从 F 到 E^* 的一个等距映射.

部分 2. 如果 $n \in \mathbf{Z}$ 而 $f \in F$, 令 $c_n(f) = \Lambda_f(e^{-2i\pi nx})$, 而 $c(f)$ 为序列 $(c_n(f))_{n\in\mathbf{N}}$.

(i) 证明 $f \mapsto c(f)$ 是从 F 到 $\ell^\infty(\mathbf{Z})$(范数为 $\| \|_\infty$) 的连续线性映射.

(ii) 证明当 $|n| \to +\infty$ 时趋向 0 的序列的空间 $\ell_0^\infty(\mathbf{Z})$ 在 ℓ^∞ 中为闭的.

(iii) 证明三角多项式的空间 Trigo 在 F 中稠密.

(iv) 由此推出 F 在 $f \mapsto c(f)$ 的像包含在 $\ell_0^\infty(\mathbf{Z})$ 中.

(v) 证明, 如果 $c(f) = 0$, 则 $\Lambda_f = 0$. 由此推出 $f \mapsto c(f)$ 为单射.

(vi) 设 $S_k(x) = \frac{\sin(2k+1)\pi x}{\sin \pi x} = \sum_{n=-k}^{k} e^{2i\pi nx}$. 证明当 $k \to +\infty$ 时, $\|c(S_k)\|_\infty = 1$, 但 $\|S_k\|_1 \to +\infty$. (可证明 $\|S_k\|_1 \geqslant \sum_{m=1}^{2k+1} \int_{(m-1)/(2k+1)}^{m/(2k+1)} \frac{|\sin(2k+1)\pi x|}{m\pi/(2k+1)} dx$.)

(vii) 由此推出从 F 到 $\ell_0^\infty(\mathbf{Z})$ 的 $f \mapsto c(f)$ 不是满的.

问题校正

部分 1. (i) $g \mapsto \Lambda_f(g)$ 的线性性由积分的线性性得到. 另外,

$$|\Lambda_f(g)| \leqslant \int_0^1 |f(t)||g(t)|dt \leqslant \|g\|_\infty \int_0^1 |f(t)|dt = \|f\|_1 \|g\|_\infty.$$

由此得到 Λ_f 的连续性 (从而它属于 E^*), 同样还有囿于上的不等式 $\|\Lambda_f\|_{E^*} \leqslant \|f\|_1$. 最后, 由于由积分的线性性得到 $f \mapsto \Lambda_f$ 的线性性, 故此囿于上的不等式证明了从 E(具有范数 $\| \|_1$) 到 E^* 的 $f \mapsto \Lambda_f$ 是连续的.

(ii) 前面的问题证明了线性映射 $f \mapsto \Lambda_f$ 是从具有 F 的范数的 E 到完备 (定理 II.1.28) 的 E^* 的连续映射. 由于 F 是 E 的完备化, 则由命题 II.1.18 的 (ii) 得到结果.

(iii) 如果 $f(x_0) = 0$, 则有 $|f(x)| < \frac{1}{2n}$, 从而在 x_0 的邻域中 $g_n(x) = 0$. 如果 $f(x_0) \neq 0$, 则 g_n 连续函数的复合的积仍然连续. 因为如果 f 是周期为 1 的周期函数, 故 g_n 也是, 于是 $g_n \in E$. 又由构造知 $\|\phi_n\|_\infty \leqslant 1$, 因此 $\|g_n\|_\infty \leqslant 1$, 并且由于当 $|f(x)| \geqslant \frac{1}{n}$ 时 $|g_n(x)| = 1$, 由此得到当 $n \geqslant \frac{1}{\|f\|_\infty}$ 时 $\|g_n\|_\infty \geqslant 1$(从而 $\|g_n\|_\infty = 1$). [586]

(iv) 当 $|f(x)| \geqslant \frac{1}{n}$ 时我们有 $h_n(x) = 0$, 而当 $|f(x)| \leqslant \frac{1}{n}$ 时则 $|h_n(x)| \leqslant |f(x)|$. 由此得到囿于上的不等式 $|h_n(x)| \leqslant \frac{1}{n}$ 和 $|\int_0^1 h_n(x)dx| \leqslant \frac{1}{n}$. 但 $|\int_0^1 h_n(x)dx| = |\|f\|_1 - \Lambda_f(g_n)|$, 从而 $|\Lambda_f(g_n)| \geqslant \|f\|_1 - \frac{1}{n}$. 由于当 n 充分大时 $\|g_n\|_\infty = 1$, 故取极限得到了囿于下的不等式 $\|\Lambda_f\|_{E^*} \geqslant 1$. 而且直接有囿于上的不等式 $\|\Lambda_f\|_{E^*} \leqslant 1$ (已经证明过), 故 $\|\Lambda_f\|_{E^*} = 1$.

(v) 由 F 的定义知 $f \mapsto \|f\|_1$ 在 F 上连续. 另外, $f \mapsto \|\Lambda_f\|_{E^*}$ 是 $f \mapsto \Lambda_f$ 和 $\Lambda \mapsto \|\Lambda\|_{E^*}$ 的复合, 其中前者是从 F 到 E^* 的连续映射, 而后者在 E^* 上连续, 故作为连续映射的复合它仍连续. 又因为这两个连续映射 $f \mapsto \|f\|_1$ 和 $f \mapsto \|\Lambda_f\|_{E^*}$ 在 E 上重合, 而 E 在 F 中稠密, 故它们相等, 这便证明了 $f \mapsto \Lambda_f$ 是从 F 到 E^* 中的一个等距映射.

部分 2. (i) $f \mapsto c(f)$ 的线性性来自 $f \mapsto \Lambda_f$ 的线性性. 又当 $n \in \mathbf{Z}$ 时有 $|c_n(f)| \leqslant \|\Lambda_f\|_{E^*}\|e^{-2i\pi nx}\|_\infty = \|f\|_1$, 因此 $\|c(f)\|_\infty \leqslant \|f\|_1$. 由此推出 $c(f)$ 属于 $\ell^\infty(\mathbf{Z})$ 以及 $f \mapsto c(f)$ 的连续性.

(ii) 设 $k \in \mathbf{N}$, 令 $c^{(k)} = (c_n^{(k)})_{n\in\mathbf{Z}}$ 是 $\ell_0^\infty(\mathbf{Z})$ 的一个序列, 它有在 $\ell^\infty(\mathbf{Z})$ 中的极限 $c = (c_n)_{n\in\mathbf{Z}}$. 令 $\varepsilon > 0$. 由于 $c^{(k)} \to c$, 故存在 k 使得 $\|c^{(k)} - c\|_\infty \leqslant \frac{\varepsilon}{2}$, 并由于 $c^{(k)} \in \ell_0^\infty(\mathbf{Z})$, 故存在 $N \in \mathbf{N}$ 使得当 $|n| \geqslant N$ 时有 $|c_n^{(k)}| \leqslant \frac{\varepsilon}{2}$. 因此有 $|c_n| \leqslant |c_n^{(k)}| + |c_n^{(k)} - c_n| \leqslant |c_n^{(k)}| + \|c^{(k)} - c\|_\infty \leqslant \varepsilon$, 这证明了当 $|n| \to +\infty$ 时 c_n 趋向 0, 因而 $c \in \ell_0^\infty(\mathbf{Z})$. 即为所证.

(iii) 设 $g \in F, \varepsilon > 0$. 由于 E 在 F 中稠密, 故存在 $f \in E$ 有 $\|g - f\|_1 \leqslant \frac{\varepsilon}{2}$. 又由于 Trigo 在 E 中稠密, 那么根据斯通 – 魏尔斯特拉斯定理 (习题 II.1.10 的 (iii)), 存在 $P \in$ Trigo 满足 $\|f - P\|_\infty \leqslant \frac{\varepsilon}{2}$. 因此 $\|f - P\|_1 = \int_0^1 |f(t) - P(t)|dt \leqslant \|f - P\|_\infty \leqslant \frac{\varepsilon}{2}$, 故 $\|g - P\|_1 \leqslant \varepsilon$. 这证明了 Trigo 在 F 中稠密.

(iv) 如果 $P \in$ Trigo, 则除了有限个 n 外 $c_n(P) = 0$; 特别地, $c(P) \in \ell_0^\infty(\mathbf{Z})$. 现在, 如果 $f \in F$, 于是存在在 F 中趋向 f 的 Trigo 中的序列 $(P_k)_{k\in\mathbf{N}}$. 由于 $g \mapsto c(g)$ 连续, 故在 $\ell^\infty(\mathbf{Z})$ 中 $c(P_k) \to c(f)$, 又由于 $\ell_0^\infty(\mathbf{Z})$ 在 $\ell^\infty(\mathbf{Z})$ 中为闭集以及每个 $c(P_k)$ 均在 $\ell_0^\infty(\mathbf{Z})$ 中, 所以作为极限的 $c(f)$ 也同样在其中.

(v) 如果 $c(f) = 0$, 则 $\Lambda_f(P) = 0$, 其中 $P \in$ Trigo. 由于 Trigo 在 E 中稠密, 而 Λ_f 在 E 上连续, 这表明 $\Lambda_f = 0$, 因此 $0 = \|\Lambda_f\|_{E^*} = \|f\|_1$, 这证明了 $f = 0$, 从而 $f \mapsto c(f)$ 的核化为 0. 得证.

(vi) 当 $|n| \leqslant k$ 时有 $c_n(S_k) = 1$, 而当 $|n| > k$ 时有 $c_n(S_k) = 0$. 由此得到 $\|c(S_k)\|_\infty = 1$. 又由于当 $t \in [0,1]$ 时有 $0 \leqslant \sin \pi t \leqslant \pi t$, 故得

$$\|S_k\|_1 = \int_0^1 \frac{|\sin(2k+1)\pi t|}{\sin \pi t}dt \geqslant \sum_{m=1}^{2k+1} \int_{(m-1)/(2k+1)}^{m/(2k+1)} \frac{|\sin(2k+1)\pi t|}{m\pi/(2k+1)}dt = \frac{2}{\pi^2}\sum_{m=1}^{2k+1}\frac{1}{m},$$

又因为 $\frac{1}{m}$ 的和发散, 便得到结论.

(vii) 如果 $f \to c(f)$ 是从 F 到 $\ell_0^\infty(\mathbf{Z})$ 上的满映射, 则 (根据 (iv)) 它是一个双射,

并 (根据 (i)) 连续, 又由于 F 和 $\ell_0^\infty(\mathbf{Z})$ 为巴拿赫空间, 它的逆也连续 (推论 II.1.26). 因此当 $c \in \ell_0^\infty(\mathbf{Z})$ 时存在 $C > 0$ 使得 $\|u(c)\|_1 \leqslant C\|c\|_\infty$. 将此结果应用于 $c = c(S_k)$ 便推出 $\|u(c(S_k))\|_1 = \|S_k\|_1 \leqslant C\|S_k\|_\infty = C$, 其中 $k \in \mathbf{N}$, 这与 (v) 矛盾.

H.6. 埃尔米特函数和在 L^2 中的傅里叶变换 [587]

这节通过构造出的 $L^2(\mathbf{R})$ 中的一个希尔伯特基给出在 $L^2(\mathbf{R})$ 中的傅里叶变换的定义.

部分 1. 设 E 是 $\mathscr{C}_c^\infty(\mathbf{R})$ 空间, 其范数为 $\|\ \|_\infty$. 赋予 E 的对偶 E^* 的范数为对偶范数 $\|\ \|_{E^*}$.

(i) 设 $f \in \mathscr{L}^1(\mathbf{R})$. 证明 $\phi \mapsto \Lambda_f(\phi) = \int_\mathbf{R} f(t)\phi(t)dt$ 定义了 E^* 中的一个只依赖于 f 在 $L^1(\mathbf{R})$ 中的像的元, 并且如此定义的 $f \mapsto \Lambda_f$ 是从 $L^1(\mathbf{R})$ 到 E^* 的连续线性映射.

(ii) 设 $f \in \mathrm{Esc}(\mathbf{R})$. 将 f 写成形如 $f = \sum_{i\in I} \alpha_i \mathbf{1}_{[\frac{k_i}{2^r}, \frac{k_i+1}{2^r}[}$, 其中 $I \subset \mathbf{Z}$ 是个有限集, 而对于 $i \in I$ 的这些 k_i 互不相同, 且 $\alpha_i \neq 0$. 设 $\phi_n : \mathbf{R} \to [0,1]$ 属于 $\mathscr{C}^\infty$, 并在 $[0,1]$ 外为 0 而在 $[\frac{1}{n}, 1-\frac{1}{n}]$ 取 1. 令 $g_n = \sum_{i\in I} \frac{\bar{\alpha}_i}{|\alpha_i|}\phi_n(2^r x - k_i)$. 证明 $\int_0^1 |1-\phi_n(t)|dt \leqslant \frac{2}{n}$. 由此推出当 $n \to +\infty$ 时, $\Lambda_f(g_n) \to \|f\|_1$ 以及 $\|\Lambda_f\|_{E^*} = \|f\|_1$.

(iii) 设 $f \in L^1(\mathbf{R})$. 证明 $\|\Lambda_f\|_{E^*} = \|f\|_1$. 由此推出, 如果对所有的 $\phi \in E$ 有 $\int_\mathbf{R} f\phi = 0$, 则 $f = 0$.

部分 2. L^1 中的傅里叶变换的单性.

(i) 设 $\phi \in E$.

(a) 设 $t_0 \in \mathbf{R}$. 证明, 如果 $\lambda > 0$, 则 $f_\lambda(x,t) = e^{-\lambda|x|}e^{-2i\pi x(t-t_0)}\phi(t)$ 在 $\mathbf{R}^2$ 上可和. 由此推出公式

$$\int_{-\infty}^{+\infty} e^{-\lambda|x|}e^{2i\pi t_0 x}\hat{\phi}(x)dx = \frac{1}{\pi}\int_\mathbf{R} \frac{\phi(t_0 + (2\pi)^{-1}\lambda u)}{1+u^2}du.$$

(b) 证明当 $\lambda \to 0$ 时, $\frac{1}{\pi}\int_\mathbf{R} \frac{\phi(t_0+(2\pi)^{-1}\lambda u)}{1+u^2}du$ 趋向 $\phi(t_0)$.

(c) 证明 $\hat{\phi}$ 可和, 且当 $\lambda \to 0$ 时, $\int_{-\infty}^{+\infty} e^{-\lambda|x|}e^{2i\pi t_0 x}\hat{\phi}(x)dx \to \overline{\mathscr{F}}\hat{\phi}(t_0)$.

(d) 证明存在 $g \in L^1(\mathbf{R})$ 使得 $\phi = \hat{g}$.

(ii) 设 $f \in L^1(\mathbf{R})$ 满足 $\hat{f} = 0$. 证明对任意的 $\phi \in E$ 有 $\int_\mathbf{R} f\phi = 0$. 由此推出 $f = 0$.

部分 3. 埃尔米特函数. 回想: 我们有 $\int_\mathbf{R} e^{-\pi t^2}dt = 1$.

(i) 证明 $(\frac{d}{dt})^n e^{-2\pi t^2} = e^{-2\pi t^2}H_n(t)$, 其中 H_n 是一个次数恰为 n 的多项式. 计算它的首项系数.

(ii) 定义 Ψ_n 为 $\Psi_n(t) = e^{-\pi t^2}H_n(t)$. 证明当 $n \neq m$ 时 $\langle \Psi_n, \Psi_m \rangle = 0$, 并计算

$\langle\Psi_n,\Psi_n\rangle$ (用分部积分法).

(iii) 证明, 如果 $\phi_1,\phi_2\in L^2(\mathbf{R})$, 则 $\phi_1\phi_2\in L^1(\mathbf{R})$.

(iv) 设 $f\in L^2(\mathbf{R})$, 并设 g 由 $g(t)=e^{-\pi t^2}f(t)$ 定义. 快速证明对任意的 $n\in\mathbf{N}$ 和 $x\in\mathbf{R}$,$t^n g(t)$ 和 $e^{2\pi|tx|}g(t)$ 可和. 由此推出, 对于 $x\in\mathbf{R}$ 有

$$\lim_{n\to+\infty}\sum_{k=0}^{n}\int_{\mathbf{R}}\frac{(-2i\pi tx)^k}{k!}g(t)dt=\hat{g}(x).$$

(v) 假设 f 与所有的 Ψ_n 均正交. 证明 $\hat{g}=0$, 从而 $f=0$.

(vi) 证明由这些 $\Psi_n(n\in\mathbf{N})$ 生成的子空间在 $L^2(\mathbf{R})$ 中稠密.

[588] (vii) 设 $e_n=(\|\Psi_n\|_2)^{-1}\Psi_n$. 如果 $f\in L^2(\mathbf{R})$, 令 $A(f)$ 为序列 $(a_n(f))_{n\in\mathbf{N}}$, 其中 $a_n(f)=\langle e_n,f\rangle$. 证明 $A(f)\in\ell^2$, 并且 A 是 $L^2(\mathbf{R})$ 到 ℓ^2 上的等距映射.

部分 4. 在 $L^2(\mathbf{R})$ 中的傅里叶变换.

(i) 证明 $\hat{\Psi}_0$ 在 $\mathbf{R}$ 上属于 $\mathscr{C}^\infty$, 并满足微分方程 $\hat{\Psi}_0'(x)=-2\pi x\hat{\Psi}_0(x)$. 由此推出 $\hat{\Psi}_0=\Psi_0$.

(ii) 证明 $\Psi_{n+1}(t)=\Psi_n'(t)-2\pi t\Psi_n(t)$. 由此推出 $\hat{\Psi}_n=(-i)^n\Psi_n$, 其中 $n\in\mathbf{N}$.

(iii) 设 σ 为映射 $(a_n)_{n\in\mathbf{N}}\mapsto((-i))^n a_n)_{n\in\mathbf{N}}$. 证明 σ 是从 ℓ^2 到 ℓ^2 上的等距映射.

(iv) 证明存在唯一的连续线性映射 $\mathscr{F}_2:L^2(\mathbf{R})\to L^2(\mathbf{R})$, 使得 $\mathscr{F}_2(\Psi_n)=\hat{\Psi}_n$, 其中 $n\in\mathbf{N}$, 并且 $\mathscr{F}_2$ 是等距的.

(v) 证明 $\mathscr{F}_2\circ\mathscr{F}_2=s$, 其中 $(s(\phi))(x)=\phi(-x)$ 几乎处处成立.

问题校正

部分 1. (i) $\phi\mapsto\Lambda_f(\phi)$ 的线性性来自积分的线性性. 现在,

$$|\Lambda_f(\phi)|\leqslant\int_0^1|f(t)||\phi(t)|dt\leqslant\|\phi\|_\infty\int_0^1|f(t)|dt=\|f\|_1\|\phi\|_\infty.$$

由此得到 Λ_f 的连续性 (因而属于 E^*) 以及囿于上的不等式 $\|\Lambda_f\|_{E^*}\leqslant\|f\|_1$. 另外, 由积分的线性性得知 $f\mapsto\Lambda_f$ 的线性性, 并且如果 f 几乎处处为 0, 则有 $\Lambda_f=0$, 这便证明了 Λ_f 只依赖于 f 在 $L^1(\mathbf{R})$ 中的像. 最后, 上面的囿于上不等式证明了 $f\mapsto\Lambda_f$ 是从 $L^1(\mathbf{R})$ (具有范数 $\|\ \|_1$) 到 E^* 的连续映射.

(ii) 不等式 $\int_0^1|1-\phi_n|\leqslant\frac{2}{n}$ 直接可得. 我们有 $(|f|-g_nf)(t)=\sum_{i\in I}|\alpha_i|(\mathbf{1}_{[0,1[}-\phi_n)(2^rt-k_i)$, 并由于 $\int_0^1|\mathbf{1}_{[0.1[}-\phi_n|\leqslant\frac{2}{n}$, 故得到 $|\int_{\mathbf{R}}|f|-g_nf|\leqslant\frac{2}{n}\sum_{i\in I}2^{-r}|\alpha_i|=\frac{2}{n}\|f\|_1$. 因为 $\int_{\mathbf{R}}(|f|-g_nf)=\|f\|_1-\Lambda_f(g_n)$, 这便证明了, 当 $n\to+\infty$ 时 $\Lambda_f(g_n)\to\|f\|_1$.

由构造知 $\|\phi_n\|_\infty=1$, 于是得到了囿于下的不等式 $\|\Lambda_f\|_{E^*}\geqslant\|f\|_1$, 并由于有显然的囿于上的不等式 $\|\Lambda_f\|_{E^*}\leqslant\|f\|_1$, 故得结论.

(iii) 按照 (i) 知 $f \mapsto \|\Lambda_f\|_{E^*}$ 在 $L^1(\mathbf{R})$ 上连续, 又由定义知 $f \mapsto \|f\|_1$ 连续. 但根据 (ii), 这两个函数在 $\mathrm{Esc}(\mathbf{R})$ 上重合, 而 $\mathrm{Esc}(\mathbf{R})$ 在 $L^1(\mathbf{R})$ 中稠密 (定理 III.2.11), 故它们在整个 $L^1(\mathbf{R})$ 上相等; 换言之, 对于任意的 $f \in L^1(\mathbf{R})$ 有 $\|\Lambda_f\|_{E^*} = \|f\|_1$. 现在, 如果对于任意的 $\phi \in E$ 有 $\int_{\mathbf{R}} f\phi = 0$, 则 $\Lambda_f = 0$, 因而 $\|\Lambda_f\|_{E^*} = 0$; 由此得到 $\|f\|_1 = 0$, 故 $f = 0$.

部分 2. (i) (a) 我们有 $|f_\lambda(x,t)| = e^{-\lambda|x|}|\phi(t)|$, 从而根据对于正函数的富比尼定理有

$$\int_{\mathbf{R}^2} |f_\lambda(x,t)| = \int_{\mathbf{R}} (\int_{\mathbf{R}} e^{-\lambda|x|}|\phi(t)|dx)dt = \int_{\mathbf{R}} \frac{2}{\lambda}|\phi(t)|dt = \frac{2}{\lambda}\|\phi\|_1 < +\infty,$$

这证明了 f_λ 可和. 因此可以两种不同的方式计算 $\int_{\mathbf{R}^2} f_\lambda$, 这给出了

$$\int_{\mathbf{R}^2} f_\lambda = \int_{\mathbf{R}} (\int_{\mathbf{R}} e^{-\lambda|x|} e^{-2i\pi x(t-t_0)} \phi(t)dt)dx = \int_{\mathbf{R}} e^{-\lambda|x|} e^{2i\pi t_0 x} \hat{\phi}(x)dx,$$

$$\int_{\mathbf{R}^2} f_\lambda = \int_{\mathbf{R}} (\int_{\mathbf{R}} e^{-\lambda|x|} e^{-2i\pi x(t-t_0)} \phi(t)dx)dt = \int_{\mathbf{R}} (\frac{1}{\lambda+2i\pi(t-t_0)} + \frac{1}{\lambda-2i\pi(t-t_0)})\phi(t)dt,$$

而结果由做变量变换 $t = t_0 + \frac{\lambda}{2\pi}u$ 得到.

(b) $\frac{\phi(t_0+(2\pi)^{-1}\lambda u)}{1+u^2}$ 按范数被 $\frac{\|\phi\|_\infty}{1+u^2}$ 控制, 而后者是可和的. 由于 $\lambda \mapsto \phi(t_0 + (2\pi)^{-1}\lambda u)$ 对于每个 $u \in \mathbf{R}$ 是连续的, 并在 $\lambda = 0$ 取 $\phi(t_0)$, 那么单参数的积分的连续性定理 (定理 IV.1.1) 便证明了, 当 $\lambda \to 0$ 时 $\frac{1}{\pi}\int_{\mathbf{R}} \frac{\phi(t_0+(2\pi)^{-1}\lambda u)}{1+u^2}du \to \frac{1}{\pi}\int_{\mathbf{R}} \frac{\phi(t_0)}{1+u^2}du = \phi(t_0)$. [589]

(c) 由于 ϕ 特别地属于 $\mathscr{C}^2$, 并具有紧支集, 故由定理 IV.2.8 得到 $(1+x^2)\hat{\phi}(x)$ 在无限远趋向 0, 又由于 $\hat{\phi}$ 连续 (定理 IV.2.7), 故其可和. 现在, 对于任意的 $\lambda > 0$, $e^{-\lambda|x|}e^{2i\pi t_0 x}\hat{\phi}(t)$ 按模被 $\hat{\phi}$ 控制, 从而由单参数积分的连续性定理得到, 当 $\lambda \to 0$ 时, $\int_{\mathbf{R}} e^{-\lambda|x|}e^{2i\pi t_0 x}\hat{\phi}(x)dx$ 趋向 $\int_{\mathbf{R}} \lim_{\lambda\to 0^+}(e^{-\lambda|x|}e^{2i\pi t_0 x}\hat{\phi}(x))dx = \int_{\mathbf{R}} e^{2i\pi t_0 x}\hat{\phi}(x)dx = \overline{\mathscr{F}}\hat{\phi}(t_0)$.

(d) 由上面得到 $\phi = \hat{g}$, 其中 g 是 $t \mapsto \phi(-t)$ 的傅里叶变换, 根据 (c) 它可和.

(ii) 如果 $\phi \in E$, 则根据 (i)(d) 知, 存在 $g \in L^1(\mathbf{R})$ 使得 $\phi = \hat{g}$. 然而, 根据命题 IV.3.24 有 $\int_{\mathbf{R}} f\phi = \int_{\mathbf{R}} f\hat{g} = \int_{\mathbf{R}} \hat{f}g$. 特别地, 如果 $\hat{f} = 0$, 则对任意的 $\phi \in E$ 有 $\int_{\mathbf{R}} f\phi = 0$. 根据部分 1 的 (iii), 它蕴含了 $f = 0$.

部分 3. (i) 如果 $(\frac{d}{dt})^n e^{-2\pi t^2} = e^{-2\pi t^2}H_n(t)$, 则 $(\frac{d}{dt})^{n+1}e^{-2\pi t^2} = e^{-2\pi t^2}H_{n+1}(t)$, 其中 $H_{n+1}(t) = H_n'(t) - 4\pi t H_n(t)$. 由于 $H_0 = 1$, 由归纳立即可得 H_n 是一个次数正好为 n 的多项式, 且其首项系数为 $(-4\pi)^n$.

(ii) 假设 $m \leqslant n$. 我们有

$$\langle \Psi_n, \Psi_m \rangle = \int_{-\infty}^{+\infty} e^{-2\pi t^2}H_n(t)H_m(t)dt = \int_{-\infty}^{+\infty} ((\frac{d}{dt})^n e^{-2\pi t^2})H_m(t)dt.$$

利用事实: 如果 P 为多项式, 则 $[P(t)e^{-2\pi t^2}]_{-\infty}^{+\infty} = 0$, 并用分部积分, 便得到

$$\langle \Psi_n, \Psi_m \rangle = -\int_{-\infty}^{+\infty} ((\frac{d}{dt})^{n-1}e^{-2\pi t^2})H_m'(t)dt = (-1)^n \int_{-\infty}^{+\infty} e^{-2\pi t^2}H_m^{(n)}(t)dt.$$

特别地, 如果 $m < n$, 则 $H_m^{(n)} = 0$ 且 $\langle \Psi_n, \Psi_m \rangle = 0$, 而如果 $m = n$, 则有 $H_m^{(n)} = n!(-4\pi)^n$, 从而 $\langle \Psi_n, \Psi_n \rangle = n!(4\pi)^n \int_{\mathbf{R}} e^{-2\pi t^2} dt = \frac{n!(4\pi)^n}{\sqrt{2}}$.

(iii) 根据柯西 – 施瓦茨不等式我们有 $\int_{\mathbf{R}} |\phi_1\phi_2| \leqslant (\int_{\mathbf{R}} |\phi_1|^2)^{1/2}(\int_{\mathbf{R}} |\phi_2|^2)^{1/2}$, 这证明了, 当 ϕ_1 和 ϕ_2 平方可和时, $\phi_1\phi_2$ 可和.

(iv) 对于 $n \in \mathbf{N}$ 时的函数 $t^n e^{-\pi t^2}$ 和对于 $x \in \mathbf{R}$ 时的 $e^{2\pi|xt|}e^{-\pi t^2}$ 是平方可和的; 利用 (iii) 由此得到 $t^n g(t)$ 和 $e^{2\pi|xt|}g(t)$ 可和. 现在,

$$|\sum_{k=0}^{n} \frac{(-2i\pi tx)^k}{k!} g(t)| \leqslant |g(t)| \sum_{k=0}^{+\infty} \frac{(2\pi|tx|)^k}{k!} = e^{2\pi|xt|}|g(t)|,$$

且由于 $t \mapsto e^{2\pi|xt|}|g(t)|$ 可和, 故可应用控制收敛定理, 从而可交换积分与取极限, 这给出了

$$\begin{aligned}\lim_{n\to+\infty} \sum_{k=0}^{n} \int_{\mathbf{R}} \frac{(-2i\pi tx)^k}{k!} g(t)dt &= \int_{\mathbf{R}} (\lim_{n\to+\infty} \sum_{k=0}^{n} \frac{(-2i\pi tx)^k}{k!}) g(t)dt \\ &= \int_{\mathbf{R}} e^{-2i\pi tx} g(t)dt = \hat{g}(x).\end{aligned}$$

(v) 由于 $\Psi_n(t) = e^{-\pi t^2} H_n(t)$, 其中 H_n 是一个次数恰等于 n 的多项式, 那么, 由这些 Ψ_n 生成的向量空间是 $e^{-\pi t^2} P(t)$ 的空间, 其中 $P(t)$ 为多项式. 因此, 如果 f 与所有的 Ψ_n 正交, 则有 $\int_{\mathbf{R}} f(t) e^{-\pi t^2} P(t) dt = \int_{\mathbf{R}} P(t) g(t) dt = 0$, 其中 P 为任意多项式. 问题 (iv) 的恒等式的左端的项因而全为零, 从而 $\hat{g} = 0$. 于是由部分 2 的问题 (ii) 得到 $g = 0$, 因此 $f = e^{\pi t^2} g = 0$.

[590] (vi) F 的闭包 $\overline{F}$ 是 $L^2(\mathbf{R})$ 中的闭集. 如果 $\overline{F}$ 严格地包含在 $L^2(\mathbf{R})$ 中, 则它的正交集非零 (参看命题 II.2.11(ii)), 这与问题 (v) 矛盾. 得到结论.

(vii) 从问题 (ii) 和 (vi) 得知, 对于 $n \in \mathbf{N}$ 的这些 e_n 构成了 $L^2(\mathbf{R})$ 的一个希尔伯特基族. 从而结果是定理 II.2.6(ii) 的直接推论.

部分 4. (i) 设 $k \in \mathbf{N}$, 而函数 $(1+t^2)^{k/2}\Psi_0(t)$ 可和, 因而 $\hat{\Psi}_0$ 属于 $\mathscr{C}^k$ (定理 IV. 2.8(ii)). 又,

$$\begin{aligned}\hat{\Psi}_0'(x) &= \int_{-\infty}^{+\infty} (-2i\pi t) e^{-2i\pi xt} e^{-\pi t^2} dt \\ &= [ie^{-\pi t^2} e^{-2i\pi xt}]_{-\infty}^{+\infty} - \int_{-\infty}^{+\infty} ie^{-\pi t^2}(-2i\pi x e^{-2i\pi xt}) dt = -2\pi x \hat{\Psi}_0(x).\end{aligned}$$

由此得到, 存在 $a \in \mathbf{C}$ 使得 $\hat{\Psi}_0(x) = ae^{-\pi x^2}$, 又由于 $\hat{\Psi}_0(0) = \int_{\mathbf{R}} e^{-\pi t^2} dt = 1$, 故有 $a = 1$, 得到结论.

(ii) $\Psi_{n+1}(t) = e^{\pi t^2}(\frac{d}{dt})^{n+1} e^{-2\pi t^2} = \frac{d}{dt}(e^{\pi t^2}(\frac{d}{dt})^n e^{-2\pi t^2}) - 2\pi t e^{\pi t^2} \left(\frac{d}{dt}\right)^n e^{-2\pi t^2} = \Psi_n'(t) - 2\pi t \Psi_n(t)$. 按照定理 IV.2.8, 我们有 $\mathscr{F}(\Psi_n')(x) = 2i\pi x \hat{\Psi}_n(x)$ 和 $\mathscr{F}(2\pi t \Psi_n(t))(x)$

$= i\hat{\Psi}'_n(x)$, 于是得到

$$\hat{\Psi}_{n+1}(x) = 2i\pi x\hat{\Psi}_n(x) - i\hat{\Psi}'_n(x) = (-i)(\hat{\Psi}'_n(x) - 2\pi x\hat{\Psi}_n(x)).$$

由此推出 $i^n\hat{\Psi}_n$ 和 Ψ_n 满足同样的递推关系, 并由于 $\hat{\Psi}_0 = \Psi_0$, 因此对于所有的 n 有 $i^n\hat{\Psi}_n = \Psi_n$. 即为所求.

(iii) 直接得到.

(iv) 唯一性来自如下事实, 即由 Ψ_n 生成的空间稠密 (部分 3, 问题 (vi)). 至于存在性, 只需令 $\mathscr{F}_2 = A^{-1} \circ \sigma \circ A$, 其中 A 是在部分 3 的问题 (vii) 中定义的映射即可: 这将 $\mathscr{F}_2$ 做成了三个满的等距映射的复合, 从而证明了 $\mathscr{F}_2$ 是从 $L^2(\mathbf{R})$ 到 $L^2(\mathbf{R})$ 上的一个等距映射.

(v) 由于 $\mathscr{F}_2 \circ \mathscr{F}_2$ 和 s 为线性连续的, 故只需证明它们在一个希尔伯特基上重合即可, 譬如对于 $n \in \mathbf{N}$ 的 e_n 这个基族. 然而根据问题 (ii), 有 $\mathscr{F}_2 \circ \mathscr{F}_2(e_n) = (-i)^n\mathscr{F}_2(e_n) = (-1)^n e_n$, 并且因为 $e^{-2\pi t^2}$ 是一个偶函数, 故有 $s(e_n) = (-1)^n e_n$, 这证明了 $\Psi_n = e^{\pi t^2}\frac{d^n}{dt^n}e^{-2\pi t^2}$ 当 n 为偶数时为偶函数, 而当 n 为奇数时为奇函数.

H.7. 傅里叶变换和卷积 [591]

本节是傅里叶 – 泊松定理的一个变形. 已知有 $\int_{\mathbf{R}} e^{-\pi x^2}dx = 1$. 在这里我们不要求去验证所遇到的函数的可测性, 按 Solovay 的话说, 这是自动满足的.

问题 1. 设 $f, g \in \mathscr{L}^1(\mathbf{R})$.

(i) 证明 $\int_{\mathbf{R}^2} |f(x-y)g(y)|dxdy = \|f\|_1\|g\|_1$.

(ii) 证明, 对几乎所有 $x \in \mathbf{R}$, 函数 $y \mapsto f(x-y)g(y)$ 可和. 定义 $f * g$ 为: 当 $\int_{\mathbf{R}} f(x-y)g(y)dy$ 收敛时 $f * g$ 等于此积分, 否则为 $f * g(x) = 0$, 于是它属于 $\mathscr{L}^1(\mathbf{R})$, 并且满足 $\|f * g\|_1 \leqslant \|f\|_1\|g\|_1$.

(iii) 证明, 如果几乎处处 $f_1 = f_2$ 和几乎处处 $g_1 = g_2$, 则几乎处处 $f_1 * g_1 = f_2 * g_2$.

(iv) 证明连续函数 $\widehat{f * g} = \hat{f}\hat{g}$. (可引进函数 $H(t,y) = e^{-2i\pi tx}f(t-y)g(y)$, 并仔细地检验计算的每个步骤的合理性.)

(v) 是否存在 $\mathscr{C}^\infty$ 类的且具有紧支集的非零函数 $\phi : \mathbf{R} \to \mathbf{R}_+$, 使得 $\hat{\phi}$ 取值于 $\mathbf{R}_+$?

问题 2. 设 $\phi_1 = \mathbf{1}_{[\frac{-1}{2}, \frac{1}{2}]}$.

(i) 证明不存在在 $\mathbf{R}$ 上的连续函数使得它几乎处处等于 ϕ_1.

(ii) 证明, 如果 $f \in \mathscr{L}^1(\mathbf{R})$, 则 $\phi_1 * f$ 是 $\mathbf{R}$ 上的一个连续函数.

(iii) 归纳定义 ϕ_k: $\phi_{k+1} = \phi_1 * \phi_k, k \geqslant 1$. 证明 ϕ_k 对 $k \geqslant 2$ 是个连续的偶函数.

(iv) 对所有的 k, 计算 $\hat{\phi}_k$. 对什么 k 函数 $\hat{\phi}_k$ 是可和的? 那么此时它的傅里叶变换是什么?

(v) 证明 ϕ_k 属于 $\mathscr{C}^{k-2}$ 类, 其中 $k \geqslant 2$.

(vi) 计算 ϕ_2. 由此得到 $\sum_{m\in\mathbf{N}} \frac{1}{(2m+1)^2}$ 的值, 从而 $\zeta(2) = \sum_{n\geqslant 1} \frac{1}{n^2}$ 的值. (可以考虑 $f(t) = \hat{\phi}_2(\frac{t}{2})$.)

(vii) 以这样的方法去证明 $\pi^{-2m}\zeta(2m) \in \mathbf{Q}$ 应该怎样做?(要求不进行计算而给出一个对策.)

问题 3. 如果 $a > 0$, 则定义 $\psi_a : \mathbf{R} \to \mathbf{R}$ 为 $\psi_a(x) = e^{-\pi a x^2}$. 注意, $\psi_a \in \mathscr{S}$.

(i) 证明 $\psi_a * \psi_b = \frac{1}{\sqrt{a+b}}\psi_{ab/(a+b)}$.

(ii) 证明 $\hat{\psi}_1(x)^k = \hat{\psi}_1(\sqrt{k}x)$, 其中 $x \in \mathbf{R}$ 和 $k \in \mathbf{N}$.

(iii) 证明 $\hat{\psi}_1$ 取实数值.

(iv) 证明存在 $a \in \mathbf{R}$ 使得 $\hat{\psi}_1(x) = e^{-\pi a x^2}$, 其中 $x \in \mathbf{R}$.

(v) 证明 $a > 0$ 从而 $a = 1$.

问题 4. (i) 证明, 如果 $|u| \leqslant 3$, 则存在 $\varepsilon > 0$ 使得 $|\frac{\sin \pi u}{\pi u}| \leqslant 1 - \varepsilon u^2$.

(ii) 证明对于所有 $k \geqslant 4, x \in \mathbf{R}$ 有 $|\hat{\phi}_k(\frac{x}{\sqrt{k}})| \leqslant \sup(e^{-\varepsilon x^2}, \frac{1}{1+x^2})$.

(iii) 设 f_k 是由 $f_k(x) = \hat{\phi}_k(\frac{x}{\sqrt{k}})$ 定义的函数, 并设 f 由 $f(x) = e^{-\frac{\pi^2 x^2}{6}}$ 给出. 证明 f_k 在 $L^1(\mathbf{R})$ 中趋向 f.

(iv) 设 g_k 是由 $g_k(x) = \sqrt{k}\phi_k(\sqrt{k}x)$ 定义的函数. 证明 g_k 在 $\mathbf{R}$ 中一致地趋向一个确定的函数 g. 这个结果对我们有什么启示吗?

[592]

问题校正

问题 1. (i) 根据对正函数的富比尼定理 (定理 III.3.3(ii)), 我们有

$$\int_{\mathbf{R}^2} |f(x-y)g(y)|dxdy = \int_{\mathbf{R}}(\int_{\mathbf{R}} |f(x-y)g(y)|dx)dy,$$

积分中的括号内在变量变换 $t = x - y$ 下给出了

$$\int_{\mathbf{R}^2} |f(x-y)g(y)|dxdy = \int_{\mathbf{R}}(\int_{\mathbf{R}} |f(t)g(y)|dt)dy = \int_{R} \|f\|_1|g(y)|dy = \|f\|_1\|g\|_1.$$

(ii) 由 (i) 知函数 $h(x,y) = f(x-y)g(y)$ 在 $\mathbf{R}^2$ 上可和, 因此按照富比尼定理 (定理 III.3.3(i)), 对几乎所有的 x 函数 $y \mapsto h(x,y)$ 在 $\mathbf{R}$ 上可和, 并且几乎处处 $x \mapsto \int_{\mathbf{R}} h(x,y)dy = f * g(x)$ 可和.

另外, 对于所有的 x 有 $|f*g(x)| \leqslant \int_{\mathbf{R}} |h(x,y)|dy$, 因而 $\|f*g\|_1 \leqslant \int_{\mathbf{R}}(\int_{\mathbf{R}} |h(x,y)|dy)dx$. 然而根据对于正函数的富比尼定理和 (i) 最后的这个量等于 $\|f\|_1\|g\|_1$.

(iii) 除了使这些积分中的一个为发散的零测度集之外, 我们有 $f_1 * g_1 - f_2 * g_2 = (f_1 - f_2) * g_1 + f_2 * (g_1 - g_2)$. 由此并利用 (ii) 得到了囿于上的不等式 $\|f_1 * g_1 - f_2 * g_2\|_1 \leqslant \|f_1 - f_2\|_1\|g_1\|_1 + \|f_2\|_1\|g_1 - g_2\|_1$. 但因为 $\|f_1 - f_2\|_1 = \|g_1 - g_2\|_1 = 0$, 故后面的项等于 0. 因已知 $\|f\|_1 = 0$ 等价于几乎处处 $f = 0$, 从而得到结果.

(iv)

$$\widehat{f*g}(x)=\int_{\mathbf{R}}e^{-2i\pi tx}f*g(t)dt=\int_{\mathbf{R}}(\int_{\mathbf{R}}e^{-2i\pi tx}f(t-y)g(y)dy)dt.$$

设 $H(t,y)=e^{-2i\pi tx}f(t-y)g(y)$. 有 $|H(t,y)|=|f(t-y)g(y)|$, 按照 (i), 这表明 H 在 $\mathbf{R}^2$ 上可和. 因此我们可利用富比尼定理得到 $\widehat{f*g}(x)=\int_{\mathbf{R}^2}e^{-2i\pi tx}f(t-y)g(y)dydt$. 做雅可比等于 1 的变量变换 $y=u,t=u+v$, 则给出了 $\widehat{f*g}(x)=\int_{\mathbf{R}^2}e^{-2i\pi(u+v)x}f(u)g(v)dudv$, 根据定理 III.3.9, 这里的被积函数可和. 最后利用公式 $e^{-2i\pi(u+v)x}=e^{-2i\pi ux}e^{-2i\pi vx}$ 和富比尼定理, 给出了

$$\widehat{f*g}(x)=\int_{\mathbf{R}}(\int_{\mathbf{R}}e^{-2i\pi ux}e^{-2i\pi vx}f(u)g(v)du)dv=\int_{\mathbf{R}}\hat{f}(x)e^{-2i\pi vx}g(v)dv=\hat{f}(x)\hat{g}(x).$$

(v) 从 $\phi_0:\mathbf{R}\to\mathbf{R}_+$ 着手, 它是一个 $\mathscr{C}^\infty$ 类的, 具有紧支集的, 不恒等于 0 的函数. 以 ϕ_1 记由 $\phi_1(x)=\phi_0(-x)$ 定义的函数, 并考虑 $\phi=\phi_0*\phi_1$. 在定义 $\hat{\phi}_1$ 的积分中做变量变换 $t\mapsto -t$ 表明有 $\hat{\phi}_1(x)=\overline{\hat{\phi}_0(x)}$, 其中 $x\in\mathbf{R}$. 由此得到 $\hat{\phi}(x)=|\hat{\phi}_0(x)|^2$ 在 $\mathbf{R}_+$ 中取值.

还需证明 ϕ 也在 $\mathbf{R}_+$ 中取值 (由于 ϕ_0 和 ϕ_1 在 $\mathbf{R}_+$ 中取值, 故由定义立即得知 ϕ 也如此) 以及 ϕ 具有紧支集 (如果 ϕ_0 在 $[-M,M]$ 外为 0, 那么 ϕ_1 也如此, 从而 $\phi_0(x-y)\phi_1(y)$ 当 $x\notin[-2M,2M]$ 时恒等于 0, 这证明了 ϕ 的支集在 $[-2M,2M]$ 中), 并且 ϕ 属于 $\mathscr{C}^\infty$ (因为 $\mathscr{S}$ 中两个函数的乘积仍在其中, 从而 $\hat{\phi}=\hat{\phi}_0\hat{\phi}_1$ 属于 $\mathscr{S}$, 那么便得到 $\overline{\mathscr{F}}\hat{\phi}$ 属于 $\mathscr{S}$; 也可以利用在和号中的求导定理 (定理 IV.1.2) 证明, 如果 $f\in\mathscr{C}_c^\infty(\mathbf{R})$, $g\in L^1(\mathbf{R})$, 则 $f*g$ 属于 $\mathscr{C}_c^\infty$).

问题 2. (i) 如果几乎处处 $g=\phi_1$, 则 $\frac{1}{2}$ 的所有邻域包含一个在其上 $g=1$ 的具有非零测度的集合 (从而非空) 以及在其上 $g=0$ 的另外一个非零测度集. 因此得到 g 不可能在 $\frac{1}{2}$ 连续.

(ii) 我们有 $\phi_1*f(x)=\int_{\mathbf{R}}h(x,y)dy$, 其中 $h(x,y)=\mathbf{1}_{[\frac{-1}{2},\frac{1}{2}]}(x-y)f(y)$. 现在,

- 除了 $y=x_0+\frac{1}{2}$ 和 $y=x_0-\frac{1}{2}$ 以外, $x\mapsto h(x,y)$ 在 x_0 连续,
- $|h(x,y)|\leqslant|f(y)|$ 可和且与 x 无关.

因此它满足定理 IV.1.1 的条件, 这便证明了 ϕ_1*f 在 x_0 连续, 而因为 x_0 任意, [593] 故它在整个 $\mathbf{R}$ 上连续.

(iii) 由 (ii) 并归纳知 ϕ_k 连续. 而由 ϕ_k 的奇偶性并在定义 $\phi_1*\phi_k(-x)$ 的积分中做变量变换 $t=-y$ 并归纳得到: 事实上, 因为 ϕ_1 和 ϕ_k 是偶函数, 故我们有 $\phi_{k+1}(-x)=\int_{\mathbf{R}}\phi_1(-x-y)\phi_k(y)dy=\int_{\mathbf{R}}\phi_1(-x+t)\phi_k(-t)dt=\int_{\mathbf{R}}\phi_1(x-t)\phi_k(t)dt$. 由于最后的这个积分等于 $\phi_{k+1}(x)$, 便证明了 ϕ_{k+1} 是偶的.

(iv) 我们有 $\hat{\phi}_1(x)=\int_{-1/2}^{1/2}e^{-2i\pi xt}dt=\frac{-1}{2i\pi x}[e^{2i\pi xt}]_{-1/2}^{1/2}=\frac{\sin\pi x}{\pi x}$. 利用问题 1 的 (iv) 进行归纳便证明了 $\hat{\phi}_k(x)=(\frac{\sin\pi x}{\pi x})^k$.

由于 $\hat{\phi}_k(k\geqslant 2)$ 连续并在无限远为 $O(\frac{1}{x^2})$, 故可和. 将在 L^1 中的傅里叶反演公式

(命题 IV.3.25) 用于 ϕ_k 给出了 $\mathscr{F}\hat{\phi}_k(x) = \phi_k(-x)$, 而由于 ϕ_k 为偶函数, 故推出了 $\hat{\phi}_k$ 的傅里叶变换是 ϕ_k.

函数 $\hat{\phi}_1$ 不是可和的. 事实上, 如果设它是可和的, 则按上面的同一论证知它的傅里叶变换就会是 ϕ_1(在 L^1 中), 并由于不存在几乎处处等于 ϕ_1 的连续函数, 这与黎曼 – 勒贝格定理矛盾.

(v) $(1+|x|^2)^{(k-2)/2}\hat{\phi}_k(x)$ 在无限远的邻域中为 $O(\frac{1}{x^2})$, 因而可和, 于是由定理 IV. 2.8(ii), $\hat{\phi}_k$ 属于 $\mathscr{C}^{k-2}$, 并由 (iv) 知这个傅里叶变换是 ϕ_k, 故得结论.

(vi) $\phi_2(x)$ 是区间 $[\frac{-1}{2}, \frac{1}{2}] \cap [x-\frac{1}{2}, x+\frac{1}{2}]$ 的长, 因而当 $|x| \geqslant 1$ 时有 $\phi_2(x) = 0$ 而当 $|x| \leqslant 1$ 时有 $\phi_2(x) = 1 - |x|$.

设 $f(t) = \hat{\phi}_2(\frac{t}{2})$. 于是 f 属于 $\mathscr{C}^1$ (甚至 $\mathscr{C}^\infty$), 而 f 和 f' 在无限远的邻域中是 $O(\frac{1}{t^2})$ 的. 因此可以将定理 IV.3.18 的泊松公式应用于它. 由于 $\hat{f}(x) = 2\mathscr{F}\hat{\phi}_2(2x) = 2\phi_2(2x)$, 这个公式变为 $2\sum_{n\in\mathbf{Z}} \phi_2(2n) = \sum_{n\in\mathbf{Z}} \hat{\phi}_2(\frac{n}{2})$. 在左端中, 唯一的非零项是 $\phi_2(0) = 1$, 而在右端, 只有 0 和奇整数有所贡献, 从而公式变为

$$2 = 1 + \sum_{n\ \text{为奇数}} \frac{1}{(\pi n/2)^2} = 1 + \frac{8}{\pi^2} \sum_{m\in\mathbf{N}} \frac{1}{(2m+1)^2},$$

故

$$\sum_{m\in\mathbf{N}} \frac{1}{(2m+1)^2} = \frac{\pi^2}{8}.$$

为了得到 $\sum_{n\geqslant 1} \frac{1}{n^2}$, 将 n 写成形如 $2^k(2m+1)$, 于是给出

$$\sum_{n\geqslant 1} \frac{1}{n^2} = \sum_{k,m\in\mathbf{N}} \frac{1}{2^{2k}} \frac{1}{(2m+1)^2} = (\sum_{k\in\mathbf{N}} \frac{1}{2^{2k}})(\sum_{m\in\mathbf{N}} \frac{1}{(2m+1)^2}) = \frac{1}{1-\frac{1}{4}} \frac{\pi^2}{8} = \frac{\pi^2}{6}.$$

(vii) 只需证明 $\phi_k(2n) \in \mathbf{Q}$ 和除了有限个 $n \in \mathbf{Z}$ 外它为 0 即可. 然而不难证明 ϕ_k 在 $[\frac{-k}{2}, \frac{k}{2}]$ 之外等于 0, 而在每个形如 $[\frac{-k}{2}+i, \frac{-k}{2}+i+1](i \in \{0, \ldots, k-1\})$ 上它是个系数在 $\mathbf{Q}$ 中的 $k-1$ 次多项式.

问题 3. (i) $\psi_a * \psi_b(x) = \int_{\mathbf{R}} e^{-\pi(a(x-t)^2+bt^2)} dt$, 但 $a(x-t)^2 + bt^2 = (a+b)(t - \frac{ax}{a+b})^2 + \frac{ab}{a+b}x^2$, 从而经变量变化 $u = \frac{1}{\sqrt{a+b}}(t - \frac{ax}{a+b})$, 并利用公式 $\int_{\mathbf{R}} e^{-\pi u^2} du = 1$ 便得到结果.

(ii) 以 ψ_1^{*k} 记 $\psi_1 * \cdots * \psi_1$ (k 个因子). 于是按照问题 1 的 (iv) 知, $\hat{\psi}_1^k$ 是 ψ_1^{*k} 的傅里叶变换. 然而由归纳并利用 (i) 可证明 $\psi_1^{*k} = \frac{1}{\sqrt{k}}\psi_{1/k}$, 并由于有 $\psi_{1/k}(x) = \psi_1(\frac{x}{\sqrt{k}})$, 故由伸缩公式便给出了结论.

(iii) ψ_1 是个偶函数, 故 $\hat{\psi}_1(x) = \int_0^{+\infty} (e^{-2i\pi xt} + e^{2i\pi xt})\psi_1(t) dt$, 这可通过在定义 $\hat{\psi}_1(x)$ 的积分中进行 $]-\infty, 0]$ 上的变量变换 $t \mapsto -t$ 得到证明. 被积函数是实的, 故得结果.

[594] (iv) 按照 (ii), 我们有 $\hat{\psi}_1(x) = \hat{\psi}_1(\frac{x}{\sqrt{k}})^k$, 其中 $k \geqslant 1$. 由于 ψ_1 属于 $\mathscr{S}$, 这表明 $\hat{\psi}_1$ 在 $\mathbf{R}$ 上属于 $\mathscr{C}^\infty$ (推论 IV.3.17). 特别地, 它在 0 有一个有限展开 $\hat{\psi}_1(x) =$

$1+\alpha x+\beta x^2+o(x^2)$ (我们有 $\hat{\psi}_1(0)=\int_{\mathbf{R}} e^{-\pi t^2}dt=1$). 对恒等式 $\hat{\psi}_1(x)=\hat{\psi}_1(\frac{x}{\sqrt{k}})^k$ 取对数, 并让 k 趋向 $+\infty$, 于是得到 $\alpha=0$ (也可由 ψ_1 是偶函数得到) 以及 $\log\hat{\psi}_1(x)=\lim_{k\to+\infty} k\log(1+\beta\frac{x^2}{k}+o(\frac{1}{k}))=\beta x^2$. 因此有 $\hat{\psi}_1(x)=e^{-\pi a x^2}$, 其中 $a=\frac{-\beta}{\pi}$.

(v) 按照黎曼 – 勒贝格定理, $\hat{\psi}_1$ 在无限远趋向 0, 从而 $a>0$. 现在, 根据在 $\mathscr{S}$ 中的傅里叶反演公式 (定理 IV.3.21), $\hat{\psi}_1$ 的傅里叶变换是 $\psi_1(-x)=\psi_1(x)$, 特别地, $1=\psi_1(0)=\int_{\mathbf{R}} e^{-\pi a x^2}=\frac{1}{\sqrt{a}}$, 因而 $a=1$. (也可注意到有

$$\beta=\frac{1}{2}\hat{\psi}_1''(0)=\frac{1}{2}\int_{\mathbf{R}}(-2i\pi t)^2 e^{-\pi t^2}dt=-4\pi^2\int_0^{+\infty}t^2e^{-\pi t^2}dt.$$

变量变换 $t=\frac{\sqrt{u}}{\sqrt{\pi}}$ 使得可以将此积分写成 $\frac{1}{2(\sqrt{\pi})^3}\int_0^{+\infty}u^{1/2}e^{-u}du=\frac{1}{2(\sqrt{\pi})^3}\Gamma(\frac{3}{2})$, 而由于 $\Gamma(\frac{3}{2})=\frac{1}{2}\Gamma(\frac{1}{2})=\frac{\sqrt{\pi}}{2}$, 故得到 $\beta=-4\pi^2\frac{1}{2(\sqrt{\pi})^3}=-\pi$, 因此 $a=1$.)

问题 4. (i) 由于 $\frac{\sin\pi u}{\pi u}$ 是偶函数, 故只需考虑 $u\in[0,3]$ 的情形. 设 $g(u)=u^{-2}(1-\frac{\sin\pi u}{\pi u})$. 于是可以令 $g(0)=\frac{\pi^2}{6}$ 将 g 连续地延拓到 0 上. 因此 g 在紧集 $[0,3]$ 上达到它的最小值 ε, 而由于当 $x>0$ 时 $\sin x<x$, 故 g 在 $\mathbf{R}_+$ 上是严格正的, 从而 $\varepsilon>0$. 如果 $u\in[0,3]$, 则 $g(u)\geqslant\varepsilon$ 便化成了我们所求的不等式.

(ii) 如果 $|x|\leqslant 3\sqrt{k}$, 则根据 (i) 有 $\hat{\phi}_k(\frac{x}{\sqrt{k}})\leqslant(1-\varepsilon\frac{x^2}{k})^k$, 又因为当 $0<u<1$ 时有 $\log(1-u)\leqslant -u$, 从而 $\hat{\phi}_k(\frac{x}{\sqrt{k}})\leqslant e^{-\varepsilon x^2}$.

如果 $|x|\geqslant 3\sqrt{k}$, 则 $|\hat{\phi}_k(\frac{x}{\sqrt{k}})|\leqslant(\frac{\sqrt{k}}{|x|})^k$. 要证明它 $\leqslant\frac{1}{1+x^2}$, 我们转向它的对数形式并做变量变换 $u=\frac{|x|}{\sqrt{k}}$. 于是这化成了证明 $k\log u-\log(1+ku^2)\geqslant 0$, 其中 $k\geqslant 4, u\geqslant 3$. 但函数 $u\mapsto k\log u-\log(1+ku^2)$ 的导数等于 $\frac{k}{u}-\frac{2ku}{1+ku^2}=\frac{k}{u(1+ku^2)}(1+(k-2)u^2)$, 而它总是正的; 于是它在 $u=3$ 达到最小, 又由于 $k\mapsto k\log 3-\log(1+9k)$ 在 $[4,+\infty[$ 上递增, 从而当 $k=4$ 时 $\geqslant 0$. 得到结论.

(iii) 在 0 的邻域中我们有 $\frac{\sin\pi u}{\pi u}=1-\frac{\pi^2u^2}{6}+o(u^2)$. 由此得到, 当 k 趋向 $+\infty$ 时 $f_k(x)=(\frac{\sin\pi x/\sqrt{k}}{\pi x/\sqrt{k}})^k$ 趋向 $e^{-\frac{\pi^2x^2}{6}}$, 又由于 f_k 被 $\sup(e^{-\varepsilon x^2},\frac{1}{1+x^2})$ 囿于上, 故它可和并与 k 无关, 那么由控制收敛定理 (定理 III.1.32) 得到 f_k 在 $L^1(\mathbf{R})$ 中趋向 $e^{-\frac{\pi^2x^2}{6}}$.

(iv) g_k 是 f_k 的傅里叶变换. 然而根据定理 IV.2.7 (黎曼 – 勒贝格定理), 这个傅里叶变换是从 $L^1(\mathbf{R})$ 到 $\mathscr{C}_0(\mathbf{R})$ (在范数 $\|\ \|_\infty$ 下) 的连续映射. 按照 (iii), f_k 在 $L^1(\mathbf{R})$ 中趋向 f, 这表明 g_k 一致地趋向 $\hat{f}$. 但 $f(t)=\psi_1(\frac{\sqrt{\pi}}{\sqrt{6}}t)$, 因此 $\hat{f}(x)=\frac{\sqrt{6}}{\sqrt{\pi}}\hat{\psi}_1(\frac{\sqrt{6}}{\sqrt{\pi}}x)=\frac{\sqrt{6}}{\sqrt{\pi}}e^{-6x^2}$. 在差一个正规化范围内, 它是中心极限定理的变化形式的一个特殊情形.

H.8. 椭圆曲线上的加法 [595]

设 (ω_1,ω_2) 是 $\mathbf{C}$ 在 $\mathbf{R}$ 上的一组正向基 ($\mathrm{Im}(\frac{\omega_2}{\omega_1})>0$), 而 $\Lambda=\{m\omega_1+n\omega_2, m,n\in\mathbf{Z}\}$. 称 $f:\mathbf{C}\to\mathbf{C}$ 是 Λ-周期的, 即对于任意的 $z\in\mathbf{C}$ 和 $\omega\in\Lambda$ 有 $f(z+\omega)=f(z)$.

部分 I.

(o) 证明存在 $C>0$ 使得对任意的 $a,b\in\mathbf{R}$ 有 $|a\omega_1+b\omega_2|\geqslant C\sup(|a|,|b|)$, 并证明 $r(\Lambda)=\inf_{\omega\in\Lambda-\{0\}}|\omega|$ 非零.

(i) 设 $A=\{\alpha\omega_1+\beta\omega_2,\alpha,\beta\in[0,1]\}$. 证明 A 为紧集并且, 如果 $z\in\mathbf{C}$, 则存在 $\omega\in\Lambda$ 和 $u\in A$ 使得 $z=\omega+u$, 由此推出, 如果 $f:\mathbf{C}\to\mathbf{R}_+$ 连续且为 Λ-周期函数, 则 f 有界并达到其最大值.

(ii) 证明一个在 $\mathbf{C}$ 上全纯且为 Λ-周期的函数是常数.

(iii) 证明当整数 $k\geqslant 3$ 时, $\sum_{\omega\in\Lambda-\{0\}}\frac{1}{\omega^k}$ 收敛.

(iv) 证明, 如果 $R>0$ 且 $|\omega|\geqslant 2R$, 则 $z+\omega$ 在 $D(0,R)$ 上不取零, 并且级数

$$\sum_{\omega\in\Lambda,|\omega|\geqslant 2R}\left(\frac{1}{(z+\omega)^2}-\frac{1}{\omega^2}\right)\quad \text{和}\quad \sum_{\omega\in\Lambda,|\omega|\geqslant 2R}\frac{1}{(z+\omega)^3}$$

在 $D(0,R)$ 上按范数收敛.

(v) 由此推出, 如果 $z\in\mathbf{C}-\Lambda$, 则级数 $F(z)=\frac{1}{z^2}+\sum_{\omega\in\Lambda-\{0\}}(\frac{1}{(z+\omega)^2}-\frac{1}{\omega^2})$ 收敛, 并且 $z\mapsto F(z)$ 在 $\mathbf{C}-\Lambda$ 上全纯[11].

(vi) 证明 F' 是 Λ-周期的, 并且 F 是个偶函数. 由此推出 F 是 Λ-周期的.

(vii) 如果 $k\geqslant 3$, 令 $G_k=\sum_{\omega\in\Lambda-\{0\}}\frac{1}{\omega^k}$. 证明级数 $\sum_{n=1}^{+\infty}(-1)^n(n+1)G_{n+2}z^n$ 的收敛半径正好是 $r(\Lambda)$, 而这个和是 $G(z)=F(z)-\frac{1}{z^2}$, 其中 $|z|<r(\Lambda)$.

(viii) 证明如果 k 为奇数, 则 $G_k=0$. 由此推出, 如果令 $g_2=60G_4$ 以及 $g_3=140G_6$, 则 $H(z)=F'(z)^2-4F(z)^3+g_2F(z)+g_3$ 全纯, 并在 0 为 0.

(ix) 证明对于任意的 $z\in\mathbf{C}-\Lambda$, 成立 $F'(z)^2=4F(z)^3-g_2F(z)-g_3$.

部分 II.

设 $\mathbf{C}/\Lambda$ 为 $\mathbf{C}$ 对于子群 Λ 的商. 回顾: 这意味着我们有一个满的群态射 $\pi:\mathbf{C}\to\mathbf{C}/\Lambda$, 使得 $\pi(z)=0$ 当且仅当 $z\in\Lambda$ (其中我们以 0 记交换群 $\mathbf{C}/\Lambda$ 的中性元). 方程 $u=-u$[12]在 $\mathbf{C}/\Lambda$ 中有 4 个解, 即 $0,e_1=\pi(\frac{\omega_1}{2}),e_2=\pi(\frac{\omega_2}{2})$ 和 $e_3=\pi(\frac{\omega_1+\omega_2}{2})$.

如果 $a\in\mathbf{C}$, 令 $S_a=\{a+\alpha\omega_1+\beta\omega_2,\alpha,\beta\in[0,1[\}$. 那么我们可以将 $\mathbf{C}$ 的每个元 z 以唯一的方式写为 $z=\omega+u$, 其中 $u\in S_a,\omega\in\Lambda$[13]. 由此得知, π 诱导了从 S_a 到 $\mathbf{C}/\Lambda$ 的一个双射, 因而 S_a 是 $\mathbf{C}/\Lambda$ 在 $\mathbf{C}$ 中的一个代表系. 以 $s_a:(\mathbf{C}/\Lambda)\to S_a$ 为这个双射的逆, 因此当 $u\in\mathbf{C}/\Lambda$ 时, $s_a(u)$ 是 u 在 S_a 中的代表.

[596] 以 $\Omega_a=\{a+\alpha\omega_1+\beta\omega_2,\alpha,\beta\in]0,1[\}$ 记 S_a 的内核, 而 γ_a 为 Ω_a 的沿正向的边

[11]标准的记号是 $\wp(z)$ 或 $\wp(z,L)$; 它是魏尔斯特拉斯 $\wp$ 函数.

[12]在 $\mathbf{C}/\Lambda$ 中它等价于 $2u=0$, 这等于说, 当提升到 $\tilde{u}\in\mathbf{C}$, $\pi(\tilde{u})=u$ 时有 $2\tilde{u}\in\Lambda$, 又或者说 $\tilde{u}\in\frac{1}{2}\Lambda$, 从而 $\frac{1}{2}\Lambda$ 中的每个元可以以唯一的方式写为形如 ω 或 $\frac{\omega_1}{2}+\omega$ 或 $\frac{\omega_2}{2}+\omega$ 或 $\frac{\omega_1+\omega_2}{2}+\omega$, 其中 $\omega\in\Lambda$.

[13]记 $z-a$ 形如 $x\omega_1+y\omega_2$, 其中 $x,y\in\mathbf{R}$, 于是 $\omega=[x]\omega_1+[y]\omega_2$, 而 $u=a+\{x\}\omega_1+\{y\}\omega_2$.

界. 它由线段 $[a, a+\omega_1], [a+\omega_1, a+\omega_1+\omega_2], [a+\omega_1+\omega_2, a+\omega_2]$ 以及 $[a+\omega_2, a]$ 组成. 注意, 我们有 $S_a \subset \mathring{\Omega}_a \cup \gamma_a$. 简单地, 以 $\int_\alpha^\beta f(z)dz$ 记积分 $\int_{[\alpha,\beta]} f(z)dz$[14].

一个 Λ-周期函数 $f: \mathbf{C} \to \mathbf{C}$ 可以看作是从 $\mathbf{C}/\Lambda$ 到 $\mathbf{C}$ 的函数. 如果 f 是 $\mathbf{C}$ 上的 Λ-周期的亚纯函数, 我们称 f 在 $\mathbf{C}/\Lambda$ 上的零点 (分别地, 极点) 是具有重数 $m_i \geqslant 1$ 的 $u_i (i \in I)$, 即 f 在 S_a 中的零点 (分别地, 极点) 是 $s_a(u_i), i \in I$, 并且 f 在 $s_a(u_i)$ 的赋值为 m_i (分别地, $-m_i$), 而这些不依赖 $a \in \mathbf{C}$ 的选取. 在这样的情形下, 我们以 $N_0(f) = \sum_{i \in I} m_i$ (分别地, $N_\infty(f) = \sum_{i \in I} m_i$) 为 f 在 $\mathbf{C}/\Lambda$ 上的零点 (分别地, 极点) 的计入重数的个数.

(i) 设 f 是 $\mathbf{C}$ 上的一个非零的亚纯函数. 证明, 如果 $a \in \mathbf{C}$, 则存在 $r_a > 0$ 使得 f 在 $D(a, r_a^-) - \{a\}$ 中既没有零点也没有极点. 由此推出, 如果 K 是 C 的一个紧集, 则 f 在 K 上只有有限个零点和有限个极点.

(ii) 如果 f 是 Λ-周期的非零函数, 且在 $\mathbf{C}$ 上亚纯. 证明存在 $a \in \mathbf{C}$ 使得 f 在道路 γ_a 上既无零点也无极点.

(iii) 证明 $\int_{\gamma_a} \frac{f'(z)}{f(z)} dz = 2i\pi(N_0(f) - N_\infty(f))$. 由此推出 $N_0(f) = N_\infty(f)$.

(iv) 此后, F 代表在部分 I 的问题 (v) 中定义的魏尔斯特拉斯函数. 计算 $N_0(F')$, 并证明 F' 是奇函数. 由此推出 F' 在 $\mathbf{C}/\Lambda$ 中的零点是 e_1, e_2 和 e_3, 而且它们是单零点.

(v) 计算 $N_\infty(F-b), b \in \mathbf{C}$. 由此推出 $F: (\mathbf{C}/\Lambda) - \{0\} \to \mathbf{C}$ 是满的, 而 $F(a) = F(a')$ 当且仅当 $a' = \pm a$. (留意 $F(a) \in \{F(e_1), F(e_2), F(e_3)\}$ 的情形.)

(vi) 推出 $z \mapsto P(z) = (F(z), F'(z))$ 是从 $(\mathbf{C}/\Lambda) - \{0\}$ 到集合 $E(C)$ 的一个双射, 其中 $E(C)$ 是方程 $Y^2 = 4X^3 - g_2 X - g_3$ 在 $\mathbf{C}^2$ 中的解 (X, Y) 的集合.

(vii) 设 $\Omega \subset \mathbf{C}$ 是一个可缩开集, 而 $f: \Omega \to \mathbf{C}$ 是在 Ω 上不取零的全纯函数. 证明存在在 Ω 上的全纯函数 g 使得 $f = e^g$, 且 $g' = \frac{f'}{f}$.

(viii) 如果 $a, b \in \mathbf{C}$, 而 $r > 0$, 并且 $\Omega_r(a,b) = \{z \in \mathbf{C}, \exists c \in [a,b], |z-c| < r\}$. 证明 $\Omega_r(a,b)$ 是一个凸开集.

(ix) 设 f 是一个非零的 Λ-周期函数, 且亚纯, 又设 $a \in \mathbf{C}$ 和 $\omega \in \Lambda$, 使得 f 在 $[a, a+\omega]$ 上既无零点也无极点. 证明, 如果 $r > 0$ 充分小, 则 f 在 $\Omega_r(a, a+\omega)$ 上既无零点也无极点. 由此推出 $\frac{1}{2i\pi} \int_a^{a+\omega} \frac{f'(z)}{f(z)} dz \in \mathbf{Z}$.

(x) 设 f 是 $\mathbf{C}$ 上的一个亚纯的非零 Λ-周期函数.

(a) 证明 S_a 中使得 $v_z(f) \neq 0$ 的元 z 的集合 X_a 有限, 并且 $\sum_{z \in X_a} v_z(f) z$ 在 $\mathbf{C}/\Lambda$ 中的像与 $a \in \mathbf{C}$ 的选取无关, 记其为 $\pi(f)$.

(b) 设 $a \in \mathbf{C}$ 使得 f 在道路 γ_a 上既无零点也无极点. 证明

$$I_1 = \frac{1}{2i\pi}\left(\int_a^{a+\omega_1} z\frac{f'(z)}{f(z)}dz + \int_{a+\omega_1+\omega_2}^{a+\omega_2} z\frac{f'(z)}{f(z)}dz\right)$$

[14] 如果 α, β 比较复杂, 则很少用它.

和

$$I_2 = \frac{1}{2i\pi}\left(\int_{a+\omega_1}^{a+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz + \int_{a+\omega_2}^{a} z\frac{f'(z)}{f(z)}dz\right)$$

属于 Λ.(仅需处理 I_1 或者 I_2.)

(c) 推出 $\pi(f) = 0$.

[597] (xi) 设 $\bar{E}(\mathbf{C}) = E(\mathbf{C}) \cup \{\infty\}$. 令 $P(0) = \infty$ 便将问题 (vi) 中的映射 $z \mapsto P(z)$ 延拓成 $\mathbf{C}/\Lambda$ 到 $\bar{E}(\mathbf{C})$ 上的一个双射, 并以 $\iota : \bar{E}(\mathbf{C}) \to \mathbf{C}/\Lambda$ 记此双射的逆. 定义 $Q_1 \oplus Q_2 (Q_1, Q_2 \in \bar{E}(\mathbf{C}))$ 为 $Q_1 \oplus Q_2 = P(\iota(Q_1) + \iota(Q_2))$. 证明 $\oplus$ 是 $\bar{E}(\mathbf{C})$ 上的交换的群运算, 其中性元为 ∞, 并且, 如果 $Q_1, Q_2, Q_3 \in E(\mathbf{C})$ 互不相同, 则 $Q_1 \oplus Q_2 \oplus Q_3 = \infty$ 当且仅当 Q_1, Q_2, Q_3 在 $\mathbf{C}^2$ 的同一条直线上. (可以关注由 $(F(z), F'(z), 1), (F(z_1), F'(z_1), 1)$ 和 $(F(z_2), F'(z_2), 1)$ 决定的函数 $G(z)$ 的零点.)

问题校正

部分 I.

(o) 映射 $(a, b) \mapsto a\omega_1 + b\omega_2$ 是 $\mathbf{R}^2$ 到 $\mathbf{C}$ 上的一个双射, 而 $(a, b) \mapsto |a\omega_1 + b\omega_2|$ 是 $\mathbf{R}^2$ 上的一个范数; 因此它等价于范数 $\|(a, b)\| = \sup(|a|, |b|)$(因为它是有限维的); 由此推出存在 $C > 0$ 使得 $|a\omega_1 + b\omega_2| \geqslant C \sup(|a|, |b|)$, 其中 $a, b \in \mathbf{R}$. 最后便有 $r(\Lambda) \geqslant C > 0$.

(i) 由于 A 是紧集 $[0, 1] \times [0, 1]$ 在连续映射 $(\alpha, \beta) \mapsto \alpha\omega_1 + \beta\omega_2$ 下的像, 故为紧集. 可以将 z 写成 $a\omega_1 + b\omega_2, a, b \in \mathbf{R}$, 那么只需令 $\omega = [a]\omega_1 + [b]\omega_2$ 而 $u = \{a\}\omega_1 + \{b\}\omega_2$ 便可得到所需要的 z 的一个形如 $z = \omega + u$ 的分解. 由此得知, 如果 f 是 Λ-周期的, 则有 $f(\mathbf{C}) = f(A)$, 又由于 A 为紧集, 加之如果 f 连续, 则表明 f 有界从而在 A 上达到它的最大值.

(ii) 如果 F 是 Λ-周期的, 且在 $\mathbf{C}$ 上全纯, 那么 $f = |F|$ 连续且是 Λ-周期的. 根据问题 (i), 这意味着 $|F|$ 达到它的最大值, 又根据刘维尔定理 (定理 V.3.11), 这表明 F 是常值.

(iii) 按照问题 (o), 我们有 $\sum_{\omega \in \Lambda - \{0\}} \frac{1}{|\omega|^k} \leqslant C^{-k} \sum_{(n,m) \in \mathbf{Z}^2 - \{(0,0)\}} \frac{1}{\sup(|m|,|n|)^k}$. 然而由于有 $8N$ 个偶对 (m, n) 满足 $\sup(|m|, |n|) = N$, 那么当 $k > 2$ 时这便给出了一个囿于上的不等式

$$\sum_{\omega \in \Lambda - \{0\}} \frac{1}{|\omega|^k} \leqslant C^{-k} \sum_{N=1}^{+\infty} \frac{8N}{N^k} \leqslant 8C^{-k}\zeta(k-1) < +\infty.$$

(iv) 我们有 $\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} = \frac{2\omega z + z^2}{\omega^2(\omega+z)^2}$ 以及当 $|\omega| \geqslant 2R$ 和 $z \in D(0, R)$ 时有 $|\omega + z| \geqslant |\omega| - |z| \geqslant \frac{|\omega|}{2}$. 特别地, $z + \omega$ 在 $D(0, R)$ 上不取零, 从而当 $z \in D(0, R)$ 和 $|\omega| \geqslant 2R$ 时有

$$\left|\frac{1}{(\omega+z)^2} - \frac{1}{\omega^2}\right| \leqslant \frac{2|\omega|R + R^2}{|\omega|^4/4} = \frac{8R}{|\omega|^3} + \frac{4R^2}{|\omega|^4}.$$

由问题 (iii) 便得到, 在 $D(0,R)$ 上的一个级数按范数收敛. 要证明第二个级数也按范数收敛, 我们注意, 当 $z\in D(0,R)$ 和 $|\omega|\geqslant 2R$ 时有 $|\frac{1}{(\omega+z)^3}|\leqslant\frac{8}{|\omega|^3}$, 从而以相同的方式得到结论.

(v) $F(z)$在$D(0,R^-)$上是每项都是在Λ外的全纯函数的有限和$\frac{1}{z^2}+\sum_{\omega\in\Lambda-\{0\},|\omega|<2R}(\frac{1}{(z+\omega)^2}-\frac{1}{\omega^2})$ 与按范数收敛的级数 $\sum_{\omega\in\Lambda,|\omega|\geqslant 2R}(\frac{1}{(z+\omega)^2}-\frac{1}{\omega^2})$ 的和, 其中后一个级数, 按照定理 V.5.1, 在 $D(0,R^-)$ 上全纯. 由此得到 F 在 $D(0,R^-)-\Lambda$ 上全纯, 因为这对任意 R 为真, 故得 F 在 $\mathbf{C}-\Lambda$ 上的全纯性.

(vi) 级数 $\frac{1}{z^2}+\sum_{\omega\in\Lambda-\{0\}}(\frac{1}{(z+\omega)^2}-\frac{1}{\omega^2})$ 的收敛性在 $\mathbf{C}-\Lambda$ 的每个紧集上是一致的, 故我们可以通过对此级数逐项求导来计算 F 的导数 (定理 V.5.1); 因此 $F'(z)=\sum_{\omega\in\Lambda}\frac{-2}{(z+\omega)^3}$. 现在, 如果 $\alpha\in\Lambda$, 则有 $F'(z+\alpha)=\sum_{\omega\in\Lambda}\frac{-2}{(z+\alpha+\omega)^3}$, 并由于这个级数绝对收敛, 故可按所要的顺序对其求和, 并且利用 $\omega\mapsto\alpha+\omega$ 是 Λ 自身的一个双射, 从而推出了 $F'(z+\alpha)=F'(z)$.

F 是偶函数来自 $(\frac{1}{(-z+\omega)^2}-\frac{1}{\omega^2})=(\frac{1}{(z-\omega)^2}-\frac{1}{(-\omega)^2})$ 以及 $\omega\mapsto-\omega$ 是 Λ 自身的一个双射.

现在, 如果 $\omega\in\Lambda$, 则函数 $F(z+\omega)-F(z)$ 的导数等于 0, 从而在 $\mathbf{C}-\Lambda$ 上是常数, 记其为 $c(\omega)$. 由于 F 为偶函数, 故有 $c(-\omega)=c(\omega)$, 而且 [598]

$$c(\omega_1+\omega_2)=F(z+\omega_1+\omega_2)-F(z+\omega_1)+F(z+\omega_1)-F(z)=c(\omega_2)+c(\omega_1).$$

令 $\omega_1=\omega,\omega_2=-\omega$, 从而得到 $2c(\omega)=0$, 因此 F 是 Λ-周期函数.

(vii) 函数 $G(z)$ 在 $\mathbf{C}-(\lambda-\{0\})$ 上全纯, 但在 $\Lambda-\{0\}$ 的每个元上是一个极点. 由 $r(\Lambda)$ 的定义知, 包含在 $\mathbf{C}-(\Lambda-\{0\})$ 中的以 0 为中心的最大开圆盘是 $D(0,r(\Lambda^-))$, 故由注记 V.4.9 得知 G 在 0 的泰勒级数的收敛半径为 $r(\Lambda)$. 现在按照 F 的定义公式知 $G(0)=0$, 并且, 根据定理 V.5.1, 可以按照导数的级数的和来计算 $G^{(n)}(0)$; 由此得到, 对 $n\geqslant 1$ 有

$$G^{(n)}(0)=\sum_{\omega\in\Lambda-\{0\}}\frac{(-1)^n(n+1)!}{\omega^{n+2}}=(-1)^n(n+1)!G_{n+2}.$$

根据注记 V.4.9 的 (i), 如果 $|z|<r(\Lambda)$, 我们有 $G(z)=\sum_{n=0}^{+\infty}\frac{G^{(n)}(0)}{n!}z^n$, 因此便得到结论.

(viii) 作为偶函数的 G, 当 k 是奇数时有 $G_k=0$, 从而

$$F(z)=\frac{1}{z^2}+3G_4z^2+5G_6z^4+O(z^5)\ \text{和}\ F'(z)=\tfrac{-2}{z^3}+6G_4z+20G_6z^3+O(z^4),$$

$$F(z)^3=\frac{1}{z^6}+\frac{9G_4}{z^2}+15G_6+O(z)\qquad\text{和}\ (F'(z))^2=\tfrac{4}{z^6}-\tfrac{24G_4}{z^2}-80G_6+O(z),$$

由此得到 $H(z)$ 可以延拓为在 0 为 0 的一个全纯函数.

(ix) $H(z)$ 是一个 Λ-周期的, 在 $\mathbf{C}-\Lambda$ 上全纯的, 并在 0 全纯的函数. 由 Λ-周期性它也在 Λ 的每个点上全纯, 从而在整个 $\mathbf{C}$ 上全纯. 根据问题 (ii) 因而它为常值, 并由于它在 0 为 0, 故其恒等于 0.

部分 II.

(i) 设 $k=v_a(f)$. 于是 $g(z)=(z-a)^{-k}f(z)$ 在 a 的邻域中全纯并在 a 非零; 因此存在 $r_a>0$ 使得 g 在 $D(a,r_a^-)$ 上不取零, 从而 f 在 $D(a,r_a^-)-\{a\}$ 上既无零点也无极点. 现在, 如果 K 为紧集, 我可以抽出 K 的覆盖 $D(a,r_a^-)(a\in K)$ 的一个有限覆盖[15]; 换言之, 存在 K 的一个有限子集 A 使得 $K\subset\cup_{a\in A}D(a,r_a^-)$. 由 r_a 的构造知, f 在 K 上的零点和极点的集合因而包含在 A 中, 故有限.

(ii) 设 $B=\{\alpha\omega_1+\beta\omega_2,\alpha,\beta\in[-1,1]\}$. 由于 B 为紧集, 故按照问题 (i), f 在 B 中只有有限个零点和极点. 当 f 在 B 中的零点和极点是 $\alpha_i\omega_1+\beta_i\omega_2,i\in I$, 其中 I 为有限集, 那么只需取 a 为形如 $\alpha\omega_1+\beta\omega_2$ 的点即可, 其中的 $\alpha\in[-1,0],i\in I$ 不是形如 α_i 或 α_i-1 的数, 而 $\beta\in[-1,0],i\in I$ 不是形如 β_i 或 β_i-1 的数.

(iii) 如果 $w\in\Omega_a$, $\frac{f'(z)}{f(z)}$ 在 w 的留数是 $v_w(f)$; 由留数公式得到 $\frac{1}{2i\pi}\int_{\gamma_a}\frac{f'(z)}{f(z)}dz=\sum_{w\in\Omega_a}v_w(f)$. 另外, 由于 f 在 $S_a-\Omega_a$ 上既无零点也无极点, 最后的这个和也等于 $\sum_{w\in S_a}v_w(f)=N_0(f)-N_\infty(f)$.

因为 $\frac{f'(z)}{f(z)}$ 是 Λ-周期的, 故有 $\int_{a+\omega_1+\omega_2}^{a+\omega_2}\frac{f'(z)}{f(z)}dz=\int_{a+\omega_1}^{a}\frac{f'(z+\omega_2)}{f(z+\omega_2)}dz=-\int_{a}^{a+\omega_1}\frac{f'(z)}{f(z)}dz$. 因此有 $\int_{a}^{a+\omega_1}\frac{f'(z)}{f(z)}dz+\int_{a+\omega_1+\omega_2}^{a+\omega_2}\frac{f'(z)}{f(z)}dz=0$ 以及 $\int_{a+\omega_1}^{a+\omega_1+\omega_2}\frac{f'(z)}{f(z)}dz+\int_{a+\omega_2}^{a}\frac{f'(z)}{f(z)}dz=0$. 于是得到 $\int_{\gamma_a}\frac{f'(z)}{f(z)}dz=0$, 从而 $N_0(f)=N_\infty(f)$.

[599] (iv) F' 有一个 3 阶极点并在 Λ 之外全纯; 因此有 $N_\infty(F')=3$. 除此之外, 因 F 是偶函数, 故 F' 是奇函数, 从而如果在 $\mathbf{C}/\Lambda$ 中 $z=-z$, 则 $F'(z)=0$. 由此得知 e_1,e_2 和 e_3 是 F' 在 $\mathbf{C}/\Lambda$ 中的零点. 由于 $N_0(F')=N_\infty(F')=3$, 这便是 F' 仅有的零点, 从而为单的.

(v) 如果 $b\in\mathbf{C}$, 函数 $F(z)-b$ 在 0 具有一个二重极点并在 Λ 之外全纯. 因此有 $N_\infty(F-b)=2$, 从而 $N_0(F-b)=2$, 这特别表明方程 $F(z)-b=0$ 在 $(\mathbf{C}/\Lambda)-\{0\}$ 的解集非空. 由此得到 $F:(\mathbf{C}/\Lambda)-\{0\}\to\mathbf{C}$ 为满射.

现在, 如果 a 是 $F(z)=b$ 的解, 那么因 F 是偶函数, 故 $-a$ 也是一个解. 由于 $N_0(F-b)=2$, 故如果 $a\neq-a$, 即如果 $a\notin\{e_1,e_2,e_3\}$, 则它们是仅有的解. 于是得到, 如果 $F(a)\notin\{F(e_1),F(e_2),F(e_3)\}$, 那么如果 $F(a')=F(a)$, 则 $a'=\pm a$.

如果 $a\in\{e_1,e_2,e_3\}$, 由于按照 (i) 有 $F'(a)=0$, 故函数 $F(z)-F(a)$ 在 $z=a$ 有二重零点, 又由于 $N_0(F(z)-F(a))=2$, 这个零点是 $F(z)-F(a)$ 在 $\mathbf{C}/\Lambda$ 中的唯一的零点; 由此又在此情形下推出 $F(a')=F(a)$ 当且仅当 $a'=\pm a$ (和 $a=-a$).

---

[15] 我们也可以 (譬如) 借助于序列进行推理: 如果 f 在 K 中的零点和极点的集合 Z 无限, 并且若 $(a_n)_{n\in\mathbf{N}}$ 是 Z 中不同元的序列, 于是可以从 $(a_n)_{n\in\mathbf{N}}$ 中抽出一个在 K 中有极限 a 的子序列, 但 $D(a,r_a^-)$ 便包含了无限多个 a_n, 这与 r_a 的定义相矛盾.

(vi) $P(z)$ 属于 $E(\mathbf{C})$ 的论断来自部分 I 的问题 (ix). 如果 $P(z_1) = P(z_2)$, 那么特别有 $F(z_1) = F(z_2)$, 从而按照 (v) 知 $z_1 = \pm z_2$. 如果 $z_1 = -z_2$, 则有 $F'(z_2) = -F'(z_1)$, 从而 $P(z_1) = P(z_2)$ 且 $z_1 \neq z_2$ 表明了 $F'(z_1) = 0$. 然而这表明 $z_1 \in \{e_1, e_2, e_3\}$, 因此 $z_1 = -z_1$ 和 $z_1 = z_2$. 由此得到了 $z \mapsto P(z)$ 是个单射. 要证明它也是个满射只要注意到, 如果 $(a,b) \in E(\mathbf{C})$, 则存在 z 使得 $F(z) = a$, 从而 $F'(z) = \pm b$, 这样, 或者 $(a,b) = P(z)$ 或者 $(a,b) = P(-z)$.

(vii) 参看命题 VI.2.3.

(viii) $\Omega_r(a,b)$ 是 $D(c, r^-)$ 对于 $c \in [a, a+\omega]$ 的并, 从而作为开集的并是个开集. 如果 $z_1, z_2 \in \Omega_r$, 则存在 $c_1, c_2 \in [a, a+\omega]$ 使得 $|z_i - c_i| < r, i = 1, 2$. 现在, 如果 $t \in [0,1]$, 则 $tc_1 + (1-t)c_2 \in [a, a+\omega]$ 和 $|(tz_1 + (1-t)z_2) - (tc_1 + (1-t)c_2)| = |t(z_1 - c_1) + (1-t)(z_2 - c_2)| < r(t + (1-t)) = r$, 这便证明了 $tz_1 + (1-t)z_2 \in \Omega_r(a,b)$, 因此 $\Omega_r(a,b)$ 是个凸集.

(ix) $\Omega_1(a, a+\omega)$ 是包含了 $[a, a+\omega]$ 的有界开集. 它的闭包 K 为紧集, 从而根据问题 (i), 只包含了 f 的有限个零点和极点. 只需取 r 为从这些零点和极点到线段 $[a, a+\omega]$ 的距离的最小值便可确信 $\Omega_r(a, a+\omega)$ 既不包含 f 的零点也不包含它的极点.

一个凸开集是可缩的, 故存在在 $\Omega_r(a, a+\omega)$ 上的全纯函数 g 使得 $e^g = f$, 因而 $g' = \frac{f'}{f}$. 于是我们有 $\int_a^{a+\omega} \frac{f'(z)}{f(z)} dz = g(a+\omega) - g(a)$, 因此又由于 f 是 Λ-周期的, 故 $\exp(\int_a^{a+\omega} \frac{f'(z)}{f(z)} dz) = f(a+\omega)/f(a) = 1$. 由此得到 $\int_a^{a+\omega} \frac{f'(z)}{f(z)} dz \in 2i\pi\mathbf{Z}$.

(x) (a) 由于在 S_a 中有界, 于是 f 在 S_a 的闭包中的零点和极点的集合有限, 当然在 S_a 中更如此. 另外, 如果将 a 换作 b, 则有 $z \mapsto s_b(\pi(z))$ 是 S_a 到 S_b 的双射, 而它诱导了从 X_a 到 X_b 的一个双射, 从而有 $z - s_b(\pi(z)) \in \Lambda$ 且 $v_z(f) = v_{s_b(\pi(z))}(f)$. 由此得到

$$\sum_{z \in X_a} v_z(f) z - \sum_{z \in X_b} v_z(f) z = \sum_{z \in X_a} v_z(f)(z - s_b(\pi(z))) \in \Lambda,$$

故 $\pi(f)$ 与 a 无关.

(b) 由于 f 是 Λ-周期的, 故 $\int_{a+\omega_1+\omega_2}^{a+\omega_2} z \frac{f'(z)}{f(z)} dz = \int_{a+\omega_1}^{a} (z + \omega_2) \frac{f'(z+\omega_2)}{f(z+\omega_2)} dz = \int_{a+\omega_1}^{a} (z + \omega_2) \frac{f'(z)}{f(z)} dz$. 由此得到 $I_1 = \frac{-1}{2i\pi} \int_a^{a+\omega_1} \omega_2 \frac{f'(z)}{fz)} dz$, 并由于 $\frac{1}{2i\pi} \int_a^{a-\omega_1} \frac{f'(z)}{f(z)} dz \in \mathbf{Z}$ (根据问题 (ix)), 我们有 $I_1 \in \mathbf{Z}\omega_2 \subset \Lambda$. 对于 I_2 的论证类似.

(c) 由 (b) 得到 $\frac{1}{2i\pi} \int_{\gamma_a} z \frac{f'(z)}{f(z)} dz = I_1 + I_2 \in \Lambda$. 另外, 由留数公式知 $\frac{1}{2i\pi} \int_{\gamma_a} z \frac{f'(z)}{f(z)} dz = \sum_{u \in \Omega_a} v_u(f) u$,, 又由于 f 在 $S_a - \Omega_a$ 上既无零点也无极点, 故有 $\sum_{u \in S_a} v_u(f) u = \sum_{u \in \Omega_a} v_u(f) u \in \Lambda$. $\sum_{u \in S_a} v_u(f) u$ 在 $\mathbf{C}/\Lambda$ 中的像 $\pi(f)$ 从而为 0.

(xi) 由构造知, $Q_1 \oplus Q_2 = Q_3$ 当且仅当 $\iota(Q_1) + \iota(Q_2) = \iota(Q_3)$. 由于 $(\mathbf{C}/\Lambda, +)$ [600] 是一个中性元为 0 的交换群, 且 ι 是 $\bar{E}(\mathbf{C})$ 到 $\mathbf{C}/\Lambda$ 的一个双射, 这意味着 $(\bar{E}(\mathbf{C}), \oplus)$ 是具有中性元 $\iota^{-1}(0) = \infty$ 的交换群.

现在, $Q_1, Q_2, Q_3 \in E(\mathbf{C})$ 互不相同并满足 $Q_1 \oplus Q_2 \oplus Q_3 = \infty$ 当且仅当 $z_1 = \iota(Q_1), z_2 = \iota(Q_2), z_3 = \iota(Q_3)$ 互不相同, 非零, 且满足 $z_1 + z_2 + z_3 = 0$. 特别有 $z_1 \neq \pm z_2$, 因此 $F_1(z_1) \neq F(z_2)$. 这表明如果将 $G(z)$ 写成 $\alpha F(z) + \beta F'(z) + \gamma$, 则由于 $\beta = F(z_2) - F(z_1)$, 故而 $\beta \neq 0$.

由于 F' 在 $z = 0$ 有一个 3 阶极点, 而 F 有一个 2 阶极点, 那么 $\beta F' + \alpha F + \gamma$ 在 $z = 0$ 恰好有 3 阶极点. 于是有 $N_\infty(G) = 3$, 由问题 (iii) 得到 G 在 $\mathbf{C}/\Lambda$ 有计重数的 3 个零点.

z_1 和 z_2 是 G 的两个显然的零点, 那么, 如果 z' 是第 3 个, 则 $\pi(G) = z_1 + z_2 + z' - 3 \cdot 0$. 于是从问题 (x) 的 (c) 得知 $z_1 + z_2 + z' = 0$, 因此 $z' = z_3$. 这便证明了 $G(z) = 0$ 当且仅当 $z \in \{z_1, z_2, z_3\}$.

另外, $\alpha X + \beta Y + \gamma = 0$ 是通过 $P(z_1) = Q_1$ 和 $P(z_2) = Q_2$ 的直线方程; 从而得到: $G(z) = 0$ 当且仅当 $P(z)$ 属于直线 (Q_1, Q_2). 证完.

[601] H.9. 解析函数的傅里叶系数

称一个函数 $f : \mathbf{R} \to \mathbf{C}$ 是解析的, 即对于每个 $a \in \mathbf{R}$, 存在 $\delta > 0$ 使得对于 $x \in]a-\delta, a+\delta[$, f 是它在 a 的泰勒级数的和. 我们打算证明一个周期函数为解析的当且仅当它的傅里叶系数的序列 $(c_n(f))_{n\in\mathbf{Z}}$ 是指数式下降的 (即存在 $r > 1$ 使得当 $|n| \to +\infty$ 时有 $|r^{|n|} c_n(f)| \to 0$.).

问题 1. (i) 证明, 如果 F 在包含 $\mathbf{R}$ 的一个开集 Ω 上全纯, 则 F 在 $\mathbf{R}$ 的限制为解析的.

(ii) 设 $(a_n)_{n\in\mathbf{Z}}$ 是使得存在 $r < 1$ 和 $C > 0$ 满足对于 $n \in \mathbf{Z}$ 有 $|a_n| \leqslant C r^{|n|}$ 的序列. 证明级数 $\sum_{n\in\mathbf{N}} a_n e^{2i\pi nt}$ 对于所有 $t \in \mathbf{R}$ 收敛并定义了 $\mathbf{R}$ 上的一个周期为 1 的解析的周期函数.

问题 2. (i) 证明, 如果 f 是 $\mathbf{R}$ 上的解析函数, 则对于每个 $a \in \mathbf{R}$ 存在一个中心为 a 的开圆盘 D_a 和一个 D_a 上的全纯函数 F_a, 使得它在 $\mathbf{R} \cap D_a$ 上的限制是 f.

(ii) 证明, 如果 $D_a \cap D_b \neq \varnothing$, 则 F_a 与 F_b 在 $D_a \cap D_b$ 上重合. 由此得到存在一个包含 $\mathbf{R}$ 的开集 Ω 和一个在其上为全纯的函数 F, 其在 $\mathbf{R}$ 上的限制等于 f.

(iii) 证明 $\mathbf{C}$ 的一个包含 $\mathbf{R}$ 的开集 Ω 包含一个形如 $\Omega(\delta) = \{z, -\delta < \mathrm{Re}(s) < 1+\delta, |\mathrm{Im}(z)| < \delta\}$ 的开矩形.

(iv) 假设 $f : \mathbf{R} \to \mathbf{C}$ 是个解析的周期为 1 的周期函数. 设 Ω 是 $\mathbf{C}$ 的一个包含 $\mathbf{R}$ 的开集, 在其上有一个限制在 $\mathbf{R}$ 上等于 f 的全纯函数 F, 而 $\delta > 0$ 使得 $\Omega(\delta)$ 包含在 Ω 中. 证明, 对于每个 $r \in]e^{-2\pi\delta}, 1[$, 存在 $C(r) > 0$ 使得对所有 $n \in \mathbf{Z}$ 有 $|c_n(f)| \leqslant C(r) r^{|n|}$.

(v) 证明结论.

问题校正

问题 1. (i) 只需回到全纯函数的定义即可: 如果 $a \in \mathbf{R}$, 则 F 只是在以 a 为中心的小圆盘上在 a 的泰勒级数的和, 那么它更是在形如 $]a-\delta, a+\delta[$ 线段上的泰勒级数的和.

(ii) 级数 $\sum_{n\in\mathbf{N}} a_n e^{2i\pi nz}$ 在带 $|\mathrm{Im}(z)| < \delta$ 中按范数收敛, 其中 $re^{2\pi\delta} < 1$ (即 $\delta < \frac{1}{2\pi}\log\frac{1}{r}$). 因为在此带形上此级数的每一项都是全纯的周期为 1 的周期函数, 故此级数在这个带形上定义了一个全纯的周期为 1 的周期函数. 它在 $\mathbf{R}$ 上的限制由 (i) 是解析的, 结论得证.

问题 2. (i) 由假设条件知, 存在 $\delta > 0$ 使得 $f(t) = \sum_{n=0}^{+\infty} \frac{f^{(n)}(a)}{n!}(t-a)^n$, 其中 $t \in]a-\delta, a+\delta[$. 特别地, 级数 $\sum_{n=0}^{+\infty} \frac{f^{(n)}(a)}{n!}T^n$ 的收敛半径 $> \delta$, 只需取 $D_a = D(a, \delta^-)$ 和 $F_a(z) = \sum_{n=0}^{+\infty} \frac{f^{(n)}(a)}{n!}(z-a)^n (z \in D_a)$ 即可.

(ii) 设 $D_a \cap D_b \neq \varnothing$, 于是 $D_a \cap D_b$ 连通 (因为凸, 从而弧连通), 那么它与 $\mathbf{R}$ 的交是一个非空开区间 I. 另外, F_a 与 F_b 在 I 上重合, 而由孤立零点定理得知 F_a 和 F_b 在整个 $D_a \cap D_b$ 上重合. 这让我们可以在 $\Omega = \cup_{a\in\mathbf{R}} D_a$ (由构造知它包含了 $\mathbf{R}$) 上定义一个函数 F: 对 $z \in D_a$ 令 $F(z) = F_a(z)$. 由于 F_a 和 F_b 在 $D_a \cap D_b$ 上重合, 从 $F(z)$ 的定义知, 尽管 $z \in D_a$, 但它并不依赖 $a \in \mathbf{R}$ 的选取. 又, F 在 D_a 上全纯, 其中 $a \in \mathbf{R}$, 因此在整个 Ω 上全纯.

(iii) 由于 $[a, b]$ 为紧集, 而 $\mathbf{C} - \Omega$ 为闭集, 又它与 $[a, b]$ 的交为空, 于是 $[a, b]$ 与 $\mathbf{C} - \Omega$ 的距离 > 0. 因此可取 $\delta = d/2$.

(iv) 由于 $f(z)e^{-2i\pi nz}$ 在 $\Omega_0 = \{z, -\delta < \mathrm{Re}(s) < 1 + \delta, |\mathrm{Im}(z)| < \delta\}$ 上全纯, 而因为为凸的, Ω_0 可缩, 故 $f(z)e^{-2i\pi nz}dz$ 在顶点为 $0, 1, 1+ic, ic$ 的矩形上的积分为 0, 其中 $c \in]-\delta, \delta[$. 又, $f(z)e^{-2i\pi nz}$ 是周期为 1 的周期函数, 在两条竖直边上的这两个积分相互抵消, 又由于在 $[0, 1]$ 上的积分正是 $c_n(f)$, 由此推出 $c_n(f) = e^{2\pi nc}\int_0^1 f(t+ic)e^{-2i\pi nt}dt$, 其中 $c \in]-\delta, \delta[$. 如果 $n \leqslant 0$, 则取 $c = \frac{-\log r}{2\pi}$, 而如果 $n \geqslant 0$ 则取 $c = \frac{\log r}{2\pi}$, 并取 $C(r) = \sup_{t\in[0,1]} \max(|f(t + i\frac{\log r}{2\pi})|, |f(t - i\frac{\log r}{2\pi}|)$, 便得到了想要的囿于上的不等式. [602]

(v) 所要的论断由问题 1 的 (ii) 与问题 2 的 (iv) 联合给出.

H.10. 级数和积分的解析延拓 [603]

本节的目的在于讲解可以容许移动积分路径的那种可塑性, 并指出该如何将这种可塑性与泊松公式结合起来, 从而可以对某些级数进行解析延拓.

如果 $s \in \mathbf{C}$, 以 $\phi_s : \mathbf{R} \to \mathbf{C}$ 记由公式 $\phi_s(t) = \frac{1}{(t^2+1)^s}$ 定义的函数, 将对数

的分支选为主分支 (回顾: 在此主分支下, 对于每个 $z \in \mathbf{C}^*$ 和 $s \in \mathbf{C}$ 有 $|z^s| \leqslant e^{\pi|\mathrm{Im}(s)|}|z|^{\mathrm{Re}(s)}$).

问题 1. 在这个问题中, s 是实的 (并在 (i) 中 $> \frac{1}{2}$, 而在 (ii)—(vi) 中 $> \frac{3}{2}$).

(i) 计算 $\int_0^{+\infty} e^{-u(1+t^2)} u^s \frac{du}{u}$. 并由此推出 $\hat{\phi}_s(0) = \frac{\sqrt{\pi}\Gamma(s-\frac{1}{2})}{\Gamma(s)}$.

(ii) 证明 $\hat{\phi}_s$ 属于 $\mathscr{C}^2$ 类, 并且 $\hat{\phi}'_s$ 是 $\frac{-2i\pi t}{(t^2+1)^s}$ 的傅里叶变换.

(iii) 证明 $\hat{\phi}_s$ 和 $\hat{\phi}'_s$ 是在无限远速降的 (回顾: f 在无限远速降是说当 $|x| \to +\infty$ 时, 对每个 $N \in \mathbf{N}$ 有 $|x^N f(x)| \to 0$).

(iv) 找出在 $\hat{\phi}_s, \hat{\phi}'_s$ 和 $\hat{\phi}''_s$ 之间的系数在 $\mathbf{C}[t]$ 中的线性关系. 由此推出 $\psi_s(x) = \hat{\phi}_s(\frac{x}{2\pi})$ 是微分方程 $x^2 v'' + 2(1-s)xv' - x^2 v = 0$ 的解.

(v) 证明 $\hat{\phi}_s$ 在 $\mathbf{R}^*$ 上属于 $\mathscr{C}^\infty$ 类, 并且它的所有导数都是速降的. 是否存在 $s > \frac{3}{2}$ 使得 $\hat{\phi}_s$ 属于 $\mathbf{R}$ 上的 $\mathscr{C}^\infty$ 类?

(vi) 考虑到 (iii) 和 (iv), 我们对于 $\hat{\phi}_s$ 在无限远的形态有什么预想? (我们只要求一个试探性的推理而非详细的对其正确性的论证.)

问题 2. 以 Ω 记从半平面 $\mathrm{Im}(s) > -1$ 去掉半直线 $[i, i\infty[$ 所得到的开集; 因为它是关于 $]-i, i[$ 每点的一个星形, 故是可缩的. 又以 $\phi_s : \Omega \to \mathbf{C}$ 记函数 $z \mapsto \frac{1}{(z^2+1)^s}$.

(i) 证明 ϕ_s 在 Ω 上全纯.

(ii) 证明, ϕ_s 可以延拓为半平面 $\mathrm{Im}(s) > -1$ 上的亚纯函数当且仅当 $s \in \mathbf{Z}$.

(iii) 设 $U_N = \{z, |\mathrm{Im}(z)| < N, |\mathrm{Re}(s)| < N\}$. 证明, 如果 $s \in U_N$, 且 $\alpha \in \mathbf{R}_+ - \{1\}$ 和 $t \in [-1,1]$, 于是有 $|\frac{1}{(1+(i\alpha+t)^2)^s}| \leqslant C_N(\alpha)$, 其中 $C_N(\alpha) = e^{\pi N} \sup(\frac{1}{|1-\alpha^2|^N}, (\alpha^4 + 4)^{N/2})$.

(iv) 证明, 如果 $s \in U_N$ 且 $t \in \mathbf{R}$, 则 $|\frac{1}{(1+(\pm 1+it)^2)^s}| \leqslant e^{\pi N}(t^4+4)^{N/2}$, 其中 $t \in \mathbf{R}$.

问题 3. 如果 $0 < \alpha < 1$, 以 γ_α 记由竖直半直线 $\gamma_{1,\alpha} =]-1+i\infty, -1+i\alpha]$, 线段 $\gamma_{2,\alpha} = [-1+i\alpha, 1+i\alpha]$ 以及竖直半直线 $\gamma_{3,\alpha} = [1+i\alpha, 1+i\infty[$ 构成的道路. 如果 $\xi < 0$, 令

$$F_\alpha(s,\xi) = \int_{\gamma_\alpha} \frac{e^{-2i\pi\xi z}}{(1+z^2)^s} dz.$$

以 $I_{1,\alpha}(s,\xi)$ (分别地, $I_{2,\alpha}(s,\xi)$, 分别地,$I_{3,\alpha}(s,\xi)$) 记在 $\gamma_{1,\alpha}$ (分别地, $\gamma_{2,\alpha}$, 分别地, $\gamma_{3,\alpha}$) 上的这个积分.

(i) 证明 $s \mapsto I_{2,\alpha}(s,\xi)$ 在整个 $\mathbf{C}$ 上全纯, 且对于每个 $\xi < 0$ 和 $s \in U_N$ 有 $|I_{2,\alpha}(s,\xi)| \leqslant 2C_N(\alpha)e^{2\pi\alpha\xi}$.

(ii) 证明 $s \mapsto I_{1,\alpha}(s,\xi)$ 和 $s \mapsto I_{3,\alpha}(s,\xi)$ 在整个 $\mathbf{C}$ 上全纯, 且存在 $C'_N(\alpha)$ 使得, 对于 $\xi \leqslant -1, s \in U_N$ 有 $|I_{1,\alpha}(s,\xi)| \leqslant C'_N(\alpha)e^{2\pi\xi\alpha}$, 其中 $i = 1, 3$. (只需处理 $I_{1,\alpha}(s,\xi)$, 因为对于 $I_{3,\alpha}(s,\xi)$ 的论证是一样的.)

[604] (iii) 证明 $s \mapsto F_\alpha(s,\xi)$ 在整个 $\mathbf{C}$ 上全纯, 并存在 $C''_N(\alpha)$ 使得对于 $\xi \leqslant -1$ 和 $s \in U_N$ 有 $|F_\alpha(s,\xi)| \leqslant C''_N(\alpha)e^{2\pi\xi\alpha}$.

问题 4. (i) 设 $f \in L^1(\mathbf{R}_+)$. 证明当 $\alpha \to +\infty$ 时 $\int_\alpha^{+\infty} |f(t)|dt \to 0$.

(ii) 证明当 $\alpha \to +\infty$ 时, $I_{1,\alpha}(s,\xi) \to 0$, 从而当 $\alpha \to +\infty$ 时 $F_\alpha(s,\xi) \to 0$.

(iii) 借助于 $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}$ 在 i 的留数推导出当 $k \in \mathbf{Z}$ 时, $F_\alpha(k,\xi)$ 的值. (当 $\alpha < \beta$ 时考虑 $F_\alpha(k,\xi) - F_\beta(k,\xi)$, 并随后讨论 α, β 和 1 的位置.)

(iv) 推导当 $k \leqslant 0$ 时 $F_\alpha(k,\xi) = 0$, 并计算当 $\alpha \in]0,1[$ 时的 $F_\alpha(s,\xi)$, 其中 $k = 1, 2$.

问题 5. 假设 $\mathrm{Re}(s) > \frac{1}{2}$, 于是 $\phi_s \in L^1(\mathbf{R})$.

(i) 证明, 对所有的 $x \in \mathbf{R}$ 有 $\hat{\phi}_s(-x) = \hat{\phi}_s(x)$.

(ii) 如果 $R > 1$, 设 $\gamma_{\alpha,R}$ 为下列的线段组成的道路: $[-R, R], [R, R+iR], [R+iR, 1+iR], [1+iR, 1+i\alpha], [1+i\alpha, -1+i\alpha], [-1+i\alpha, -1+iR], [-1+iR, -R+iR]$ 和 $[-R+iR, -R]$. $e^{-2i\pi\xi z}\phi_s(z)dz$ 沿此道路的积分等于多少? 由此推出 $F_\alpha(s,\xi) = \hat{\phi}_s(\xi)$, 其中 $\alpha \in]0,1[$.

(iii) 证明在无限远的邻域中, 对于 $\alpha \in]0,1[$ 有 $\hat{\phi}_s(\xi) = O(e^{-2\pi\alpha|\xi|})$. 它是否与我们在问题 1 的 (vi) 中所试探的结果一致?

问题 6. (i) 证明 $\sum_{n\in\mathbf{Z}} \frac{1}{n^2+1} = \pi\frac{1+e^{-2\pi}}{1-e^{-2\pi}}$ 和 $\sum_{n\in\mathbf{Z}} \frac{1}{(n^2+1)^2} = \frac{\pi}{2}\frac{1+e^{-2\pi}}{1-e^{-2\pi}} + 2\pi^2\frac{e^{-2\pi}}{(1-e^{-2\pi})^2}$.

(ii) 证明级数 $\sum_{n=1}^{+\infty} F_{1/2}(s,-n)$ 对所有 $s \in \mathbf{C}$ 收敛, 且其和 $F(s)$ 是整个 $\mathbf{C}$ 上的全纯函数.

(iii) 证明 $G(s) = \sum_{n\in\mathbf{Z}} \frac{1}{(n^2+1)^s}$ 在 $\mathrm{Re}(s) > \frac{1}{2}$ 上收敛并在此半平面上全纯.

(iv) 证明 G 有到整个 $\mathbf{C}$ 上的亚纯延拓, 其在 $-k + \frac{1}{2}(k \in \mathbf{N})$ 上有单极点, 除此之外它是全纯的.

(v) 如果 $k \in \mathbf{N}$, 那么 $G(-k)$ 是什么?

问题 7. (i) 设 $f : [0,1] \to \mathbf{R}_+^*$ 属于 $\mathscr{C}^\infty$, 并设 $a, b \in \mathbf{R}, a > 0$. 证明函数 $s \mapsto \int_0^1 t^{as+b} f(t)^s dt$ 可延拓成整个 $\mathbf{C}$ 上的亚纯函数并且除了在 $\frac{-b-k}{a}(k \in \mathbf{N} - \{0\})$ 可能有的单极点外全纯. (可以利用对 $t \mapsto f(t)^s$ 的具有 n 阶积分余项的泰勒公式.)

(ii) 设 P 是个实系数的 $d \geqslant 2$ 次的首 1 多项式, 其在 $\mathbf{R}$ 上不取零. 证明 $\int_{-\infty}^{+\infty} \frac{1}{P(t)^s} dt$ 可延拓为整个 $\mathbf{C}$ 上的一个亚纯函数, 并除了在 $\frac{1-k}{d}(k \in \mathbf{N})$ 上的可能的单极点外全纯.

(iii) 设 α (分别地, A) 为 $|\mathrm{Im}(a)|$ 的最小值 (分别地, $|\mathrm{Re}(a)|$ 的最大值), 其中 a 是 P 的根. 令 Ω^+ 是从半平面 $\mathrm{Re}(s) > -\alpha$ 去掉闭带 $\{z, |\mathrm{Re}(z)| \leqslant A, \mathrm{Im}(z) \geqslant \alpha\}$ 得到的开集, 而 Ω^- 是 Ω^+ 相对于实轴的对称集合. 证明 $z \mapsto \frac{1}{P(z)^s}$ 可延拓为 Ω^+ 上和 Ω^- 上的全纯函数 $\phi_{P,s}$. (可以将 P 分解因子并化到 ϕ_s.)

(iv) 证明 $G_P(s) = \sum_{n\in\mathbf{Z}} \frac{1}{P(n)^s}$ 可以延拓为整个 $\mathbf{C}$ 上的亚纯函数, 并除了在 $\frac{1-k}{d}(k \in \mathbf{N})$ 上的可能的单极点外全纯.

[605] 问题校正

问题 1. (i) 变量变换 $v=(1+t^2)u$ 给出了公式 $\int_0^{+\infty} e^{-u(1+t^2)}u^s\frac{du}{u}=\frac{\Gamma(s)}{(1+t^2)^s}$. 由此得到 $\hat{\phi}_s(0)=\frac{1}{\Gamma(s)}\int_{-\infty}^{+\infty}(\int_0^{+\infty} e^{-u(1+t^2)}u^s\frac{du}{u})dt$.

于是可以利用对于正函数的富比尼定理交换这两个积分, 并由于 $\int_{-\infty}^{+\infty} e^{-u(1+t^2)}dt=e^{-u}\int_{-\infty}^{+\infty}e^{-ut^2}dt=\sqrt{\frac{\pi}{u}}e^{-u}$ (变量变换 $t=\sqrt{\frac{\pi}{u}}v$ 将其化到了高斯积分), 让我们最后得到 $\hat{\phi}_s(0)=\frac{\sqrt{\pi}}{\Gamma(s)}\int_0^{+\infty}e^{-u}u^{s-\frac{1}{2}}\frac{du}{u}=\frac{\sqrt{\pi}\Gamma(s-\frac{1}{2})}{\Gamma(s)}$.

(ii) 函数 $t\mapsto(1+t^2)\phi_s(t)$ 可和, 故由定理 IV.2.8 得到结果.

(iii) 由归纳立即可知 ϕ_s 的 k 阶导数具有 $t\mapsto\frac{P_k(t)}{(t^2+1)^{s+k}}$ 形式, 其中 P_k 是一个 k 次多项式; 因此它对于所有的 k 都可和, 这便让我们可以利用定理 IV.2.8 的 (i) 得到, 对于每个 $k\in\mathbf{N}$, 在无限远有 $x^k\hat{\phi}_s\to 0$. 于是对 $\hat{\phi}_s$ 得到了结论. 至于对于 $\hat{\phi}'_s$ 的推理是完全一样的: $t\phi_s(t)$ 的 k 阶导数具有 $\frac{Q_k(t)}{(t^2+1)^{s+k}}$ 形式, 其中 Q_k 是个 $k+1$ 次多项式; 因而它对所有的 k 可和.

(iv) 我们有 $(t^2+1)\phi''_s+2(s+1)t\phi'_s+2s\phi_s=0$. 由此得到

$$(-\frac{d^2}{dx^2}+1)(-x^2\psi_s)+2(s+1)\frac{-id}{dx}(-ix\psi_s)+2s\psi_s=0.$$

结果直接由计算得到.

(v) $\hat{\phi}_s$ 满足的这个微分方程可归纳地用来证明 $\hat{\phi}_s$ 在 $\mathbf{R}^*$ 上是 $\mathscr{C}^k$ 类的, 并且 $\hat{\phi}_s^{(k)}$ 是 $\hat{\phi}_s$ 和 $\hat{\phi}'_s$ 的系数在 $\mathbf{C}[\frac{1}{x}]$ 中的线性组合. 由于 $\hat{\phi}_s$ 和 $\hat{\phi}'_s$ 在无限远速降, 故 $\hat{\phi}_s^{(k)}$ 对于任意的 k 也如此.

如果 $\hat{\phi}_s$ 在 $\mathbf{R}$ 上属于 $\mathscr{C}^\infty$, 则它属于施瓦兹空间, 因而它的反演傅里叶变换也如此 (推论 IV.3.17). 另外, 由于 ϕ_s 和 $\hat{\phi}_s$ 在 L^1 中, 那么 $\hat{\phi}_s$ 的反演傅里叶变换便是 ϕ_s (命题 IV.3.25). 由于 ϕ_s 不是速降的, 它便引出了矛盾, 从而证明了 $\hat{\phi}_s$ 在 $\mathbf{R}$ 上不是 $\mathscr{C}^\infty$ 的.

(vi) 在无限远的邻域中, $\hat{\phi}_s$ 所满足的这个微分方程趋向微分方程 $v''=4\pi^2v$, 它的解空间的基由 $e^{2\pi x}$ 和 $e^{-2\pi x}$ 组成. 在此方程 $v''=4\pi^2v$ 的解中只有 $e^{-2\pi x}$ (分别地, $e^{2\pi x}$) 的倍数不会膨胀到 $+\infty$ (分别地, $-\infty$); 于是我们预料 $\hat{\phi}_s$ 在 $+\infty$ 的邻域与 $e^{-2\pi x}$ 的倍数相像, 而在 $-\infty$ 的邻域与 $e^{2\pi x}$ 的倍数相像.

事实上, 我们有 $\frac{\Gamma(s)}{\pi^s}\hat{\phi}_s(x)=|x|^{s-\frac{1}{2}}K_{s-\frac{1}{2}}(2\pi|x|)$, 其中 K_ν 是在习题 IV.1.9 中的贝塞尔函数, 它由公式 $K_\nu(y)=\frac{1}{2}\int_0^{+\infty}e^{-y(t+t^{-1})/2}t^\nu\frac{dt}{t}$ 给出, 其中 $\nu\in\mathbf{C}, y\in\mathbf{R}_+^*$, 于是可以利用这个习题的 (ii) 在无限远的邻域中得到 $\hat{\phi}_s$ 的一个等价的表示. 前面的公式来自下面的计算, 其中我们逐次地利用了 (i), 富比尼定理, e^{-ut^2} 的傅里叶变换是 $\sqrt{\frac{\pi}{u}}e^{u^{-1}\pi^2x^2}$ 这个结果和变量变换 $u=\pi|x|w$:

$$\begin{aligned}\hat{\phi}_s(x)&=\int_{\mathbf{R}}\frac{1}{(t^2+1)^s}e^{-2i\pi tx}dt=\frac{1}{\Gamma(s)}\int_{\mathbf{R}}\int_0^{+\infty}e^{-u(t^2+1)}u^se^{-2i\pi tx}\frac{du}{u}dt\\&=\frac{1}{\Gamma(s)}\int_0^{+\infty}e^{-u}u^s\frac{du}{u}\int_{\mathbf{R}}e^{-ut^2}e^{-2i\pi tx}dt\end{aligned}$$

$$= \frac{\sqrt{\pi}}{\Gamma(s)} \int_0^{+\infty} e^{-u-u^{-1}\pi^2 x^2} u^{s-\frac{1}{2}} \frac{du}{u}$$
$$= \frac{\pi^s}{\Gamma(s)} |x|^{s-\frac{1}{2}} \int_0^{+\infty} e^{-2\pi|x|(w+w^{-1})} w^{s-\frac{1}{2}} \frac{dw}{w}.$$

问题 2. (i) Ω 在 $z \mapsto z^2+1$ 下的像在 $\mathbf{C}-\mathbf{R}_-$ 之中, 而 ϕ_s 是从 Ω 到 $\mathbf{C}-\mathbf{R}_-$ 的映射 $z \mapsto z^2+1$ 与从 $\mathbf{C}-\mathbf{R}_-$ 到 $\mathbf{C}$ 中的映射 $z \mapsto \exp(s\log z)$ 的复合, 其中每一个都全纯, 由此推出 ϕ_s 是全纯的. [606]

(ii) 如果 $s \in \mathbf{Z}$, 则函数 $z \mapsto \frac{1}{(z^2+1)^s}$ 作为两个全纯函数的商在整个 $\mathbf{C}$ 上亚纯 (甚至在 $s<0$ 全纯).

另外, 如果 $a>1$ 且 ε 趋向 0, 则 $(ia+\varepsilon)^2+1 = 1+\varepsilon^2-a^2+2ia\varepsilon$ 趋向一个负数, 而这个数本身满足当 $\varepsilon>0$ 时其虚部为正, 而当 $\varepsilon<0$ 时为负. 由此得到 $\log(z^2+1)$ 在 $ia+0^+$ 和 $ia+0^-$ 的极限不同于 $2i\pi$, 从而 $\frac{1}{(z^2+1)^s}$ 的这两个极限不同于 $e^{-2i\pi s}$ 的某个倍数, 而当 $s \notin \mathbf{Z}$ 时它不等于 1. 因此我们不能将 ϕ_s 连续地延拓到半直线 $[i, i\infty]$ 上的任何点上, 故 ϕ_s 不能延拓到 $\mathrm{Im}(s)>-1$ 的严格包含了 Ω 的任一个开集上.

(iii) 我们有 $|1+(i\alpha+t)|^2 = (1-\alpha^2)^2+t^4+2t^2+2t^2\alpha^2$, 因此, 如果 $|t| \leqslant 1$, 则 $(1-\alpha^2)^2 \leqslant |1+(i\alpha+t)|^2 \leqslant \alpha^4+4$. 于是得到 $|\frac{1}{(1+(i\alpha+t)^2)^s}| \leqslant e^{\pi|\mathrm{Im}(s)|}\sup(\frac{1}{|1-\alpha^2|^{\mathrm{Re}(s)}}, (\alpha^4+4)^{\mathrm{Re}(s)/2})$, 结论则来自 s 属于 U_N 这个假设条件.

(iv) 有 $|1+(\pm1+it)^2|^2 = t^4+4$, 从而 $|\frac{1}{(1+(\pm1+it)^2)^s}| \leqslant \frac{e^{\pi|\mathrm{Im}(s)|}}{(t^4+4)^{\mathrm{Re}(s)/2}}$, 结论也来自 s 属于 U_N.

问题 3. (i) 设 $g(t,s) = \frac{e^{-2i\pi\xi(i\alpha+t)}}{(1+(i\alpha+t)^2)^s}$, 从而 $I_{2,\alpha}(s,\xi) = -\int_{-1}^1 g(t,s)dt$.

- 如果固定 $t \in [-1,1]$, 则 $s \mapsto g(t,s)$ 在 U_N 上全纯.
- 根据问题 2 的 (iii), 如果 $t \in [-1,1], s \in U_N$, 则有 $|g(t,s)| = \frac{e^{2\pi\xi\alpha}}{|(1+(i\alpha+t)^2)^s|} \leqslant C_N(\alpha)e^{2\pi\xi\alpha}$.

由于 $t \mapsto C_N(\alpha)e^{2\pi\xi\alpha}$ 在 $[-1,1]$ 上可和, 于是它满足定理 V.5.7 的那个映射的条件, 从而证明了 $s \mapsto I_{2,\alpha}(s,\xi)$ 在 U_N 上全纯. 又由于这对任意的 N 为真, 故也就在 $\cup_{N\in\mathbf{N}} U_N = \mathbf{C}$ 上全纯.

最后, $|I_{2,\alpha}(s,\xi)| \leqslant \int_{-1}^1 |g(s,t)|dt \leqslant 2C_N(\alpha)e^{2\pi\xi\alpha}$, 故有结论.

(ii) 设 $g(t,s) = \frac{e^{-2i\pi\xi(-1+it)}}{(1+(-1+it)^2)^s}$, 故有 $I_{1,\alpha}(s,\xi) = -\int_\alpha^{+\infty} g(t,s)dt$.

- 如果固定 $t \in [\alpha,+\infty[$, 则 $s \mapsto g(t,s)$ 在 U_N 上可和.
- 对于 $t \in [\alpha,+\infty[, s \in U_N$, 则有 $|g(t,s)| = \frac{e^{2\pi\xi t}}{|(2-t^2-2it)^s|} \leqslant \frac{e^{\pi|\mathrm{Im}(s)|}e^{2\pi\xi t}}{(t^2+4)^{\mathrm{Re}(s)/2}} \leqslant e^{\pi N}(t^4+4)^{N/2}e^{2\pi\xi t}$.

由于 $\xi<0$, 函数 $t \mapsto e^{\pi N}(t^4+4)^{N/2}e^{2\pi\xi t}$ 在 $[\alpha,+\infty[$ 上可和, 因而满足了定理 V.5.7 中的假设条件, 便证明了 $s \mapsto I_{1,\alpha}(s,\xi)$ 在 U_N 上全纯, 由于这对于所有 N 为真, 故它也在 $\cup_{N\in\mathbf{N}} U_N = \mathbf{C}$ 上为真.

最后, $|I_{1,\alpha}(s,\xi)| \leqslant \int_\alpha^{+\infty} |g(t,s)|dt \leqslant \int e^{2\pi\xi\alpha}\int_0^{+\infty} e^{\pi N}((t+\alpha)^4+4)^{N/2}e^{2\pi\xi t}dt$, 且

由于假设了 $\xi \leqslant -1$, 故此积分可以以 $C_N'(\alpha) = \int_0^{+\infty} e^{\pi N}((t+\alpha)^4+4)^{N/2}e^{-2\pi t}dt$ 为强函数, 这证明了结论.

(iii) 由于 $F_\alpha(s,\xi) = \sum_{i=1}^3 I_{i,\alpha}(s,\xi)$, 这便是 (i) 和 (ii) 的直接推论, 从而可取 $C_N''(\alpha) = 2C_N(\alpha) + 2C_N'(\alpha)$.

问题 4. (i) 如果 α_n 是一个趋向 $+\infty$ 的序列, 且若 $f_n(t) = f(t)\mathbf{1}_{[\alpha_n,+\infty[}(t)$, 则 f_n 在绝对值上被 $|f|$ 囿于上, 并在 $[0,+\infty[$ 中每点 $f_n \to 0$. 根据控制收敛定理, 对任意趋向 0 的序列, $\int_{\alpha_n}^{+\infty} f = \int_0^{+\infty} f_n \to 0$, 故得结论.

(ii) $I_{1,\alpha}(s,\xi)$ 是可和函数 $g(t) = \frac{e^{-2i\pi\xi(-1+it)}}{(1+(-1+it)^2)^s}$ 在 $[\alpha,+\infty[$ 上的积分; 由此得到, 当 $\alpha \to +\infty$ 时 $I_{1,\alpha}(s,\xi) \to 0$.

现在, $F_\alpha(s,\xi) = I_{1,\alpha}(s,\xi) + I_{2,\alpha}(s,\xi) + I_{3,\alpha}(s,\xi)$. 利用证明 $I_{1,\alpha}(s,\xi) \to 0$ 的论证可证明 $I_{3,\alpha}(s,\xi) \to 0$. 最后, 当 $s \in U_N$ 时有 $|I_{2,\alpha}(s,\xi)| \leqslant C_N(\alpha)e^{2\pi\xi\alpha}$, 而当 $\alpha \to +\infty$ 时有 $C_N(\alpha) = e^{\pi N}(\alpha^4+4)^{N/2}$. 因为 $\xi < 0$, 故 $(\alpha^4+4)^{N/2}e^{2\pi\xi\alpha} \to 0$. 得到结论.

(iii) 如果 $\alpha < \beta$, 则 $F_\alpha(k,\xi) - F_\beta(k,\xi)$ 是 $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}dz$ 的积分, 其积分路径是顶点为 $-1+i\alpha, 1+i\alpha, 1+i\beta, -1+i\beta$ 的矩形. 由于 $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}dz$ 在去掉 i 的半平面 $\mathrm{Im}(s) > -1$ 上全纯, 故留数公式证明, 当 $\alpha < \beta < 1$ 或 $1 < \alpha < \beta$ 时有 $F_\alpha(k,\xi) - F_\beta(k,\xi) = 0$, 而当 $\alpha < 1 < \beta$ 时有 $F_\alpha(k,\xi) - F_\beta(k,\xi) = 2i\pi\mathrm{Res}(\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}, i)$. 特别地, $\alpha \mapsto F_\alpha(k,\xi)$ 在 $]1,+\infty[$ 上为常值, 并因为 $\alpha \to +\infty$ 时 $F_\alpha(k,\xi) \to 0$, 故对于 $\alpha > 1$ 有 $F_\alpha(k,\xi) = 0$, 而当 $\alpha < 1$ 时 $F_\alpha(k,\xi) = 2i\pi\mathrm{Res}(\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}, i)$. [607]

(iv) 如果 $k \leqslant 0$, 函数 $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}$ 在 $z = i$ 为全纯的, 从而其留数为 0, 故 $F_\alpha(k,\xi) = 0$.

如果 $k = 1$, 函数 $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}$ 在 $z = i$ 有一个单极点, 其留数为 $\lim_{z\to i}(z-i)\frac{e^{-2i\pi\xi z}}{(1+z^2)} = \lim_{z\to i}\frac{e^{-2i\pi\xi z}}{z+i} = \frac{1}{2i}e^{2\pi\xi}$. 从而有 $F_\alpha(1,\xi) = \pi e^{2\pi\xi}$.

如果 $k = 2$, 则函数 $\frac{e^{-2i\pi\xi z}}{(1+z^2)^k}$ 在 $z = i$ 有一个 2 阶极点, 其留数是 $\frac{e^{-2i\pi\xi z}}{(1+z^2)^2}$ 在 $z = i$ 的泰勒展开式的一次项的系数. 由于

$$\frac{e^{-2i\pi\xi z}}{(z+i)^2} = \frac{e^{2\pi\xi}(1-2i\pi\xi(z-i)+\cdots)}{-4+4i(z-i)+\cdots} = \frac{-1}{4}e^{2\pi\xi}(1+(i-2i\pi\xi)(z-i)+\cdots),$$

从而有 $F_\alpha(2,\xi) = 2i\pi\cdot\frac{-1}{4}(i-2i\pi\xi)e^{2\pi\xi} = (\frac{\pi}{2}-\pi^2\xi)e^{2\pi\xi}$.

问题 5. (i) 此结果来自变量变换 $u = -t$ 以及 ϕ_s 的奇偶性.

(ii) 由于 $\gamma_{\alpha,R}$ 是一个包含在 Ω 内的闭道, 而 Ω 是可缩的, 故 $e^{2\pi\xi z}\phi_s(z)dz$ 沿此道路的积分等于 0, 其中对所有的 R. 在 $[R,R+iR], [R+iR,1+iR], [-1+iR,-R+iR]$ 和 $[-R+iR,-R]$ 中每个线段上, 我们有 $|z^2+1| \geqslant R^2-1$ 和 $|e^{2\pi\xi z}| \leqslant 1$, 因此 $|e^{2\pi\xi z}\phi_s(z)| \leqslant \frac{e^{\pi|\mathrm{Im}(s)|}}{(R^2-1)^{\mathrm{Re}(s)}}$. 另外, 这四条线段的长 $\leqslant R$, 因此在这些线段上的积分和的绝对值被 $\frac{4Re^{\pi|\mathrm{Im}(s)|}}{(R^2-1)^{\mathrm{Re}(s)}}$ 囿于上, 故当 R 趋向 $+\infty$ 时, 因 $\mathrm{Re}(s) > \frac{1}{2}$ 而趋向 0. 由于在 $[-R,R]$ 上的积分趋向 $\hat{\phi}_s(\xi)$, 并由于在剩下的三段上的积分和趋向 $-F_\alpha(s,\xi)$, 故得结论.

(iii) 是问题 3(iii) 的直接推论.

问题 6. (i) 函数 $\frac{1}{1+t^2}$ 连同它的导数 $\frac{-2t}{(1+t^2)^2}$ 都可和; 因此可将泊松公式用于它, 那么利用公式 $\hat{\phi}_1(n)=\pi e^{-2\pi|n|}$, 问题 5 的 (ii) 和问题 4 的 (iv) (对 $n<0$) 的结果以及 $\hat{\phi}_1$ 的奇偶性 (为了得到 >0 的情形) 我们得到:

$$\sum_{n\in\mathbf{Z}}\frac{1}{1+n^2}=\pi+2\pi\sum_{n=1}^{+\infty}e^{-2\pi n}=\pi(1+2\frac{e^{-2\pi}}{1-e^{-2\pi}})=\pi\frac{1+e^{-2\pi}}{1-e^{-2\pi}}.$$

同样地,

$$\sum_{n\in\mathbf{Z}}\frac{1}{(1+n^2)^2}=\hat{\phi}_2(0)+2\sum_{n=1}^{+\infty}F_{1/2}(2,-n)=\frac{1}{2}\pi+2\sum_{n=1}^{+\infty}(\frac{\pi}{2}+\pi^2n)e^{-2\pi n}.$$

于是通过对恒等式 $\frac{1}{1-z}=\sum_{n=0}^{+\infty}z^n$ 求导得到的公式 $\sum_{n=0}^{+\infty}nz^n=\frac{z}{(1-z)^2}$ 便给出了结论.

(ii) 按照问题 3 的 (iii)(用于 $\alpha=\frac{1}{2}$ 的情形), 对于所有 $n\geqslant 1$ 及 $s\in U_N$ 有 $|F_{1/2}(s,-n)|\leqslant C''_N(\frac{1}{2})e^{-\pi n}$. 由此得到级数 $\sum_{n=1}^{+\infty}F_{1/2}(s,-n)$ 在 U_N 上按模收敛, 又由于它的每一项在整个 $\mathbf{C}$ 上全纯 (问题 3 的 (iii)), 故根据定理 V.5.1, 它的和 $F(s)$ 在 U_N 上全纯. 由此推出 F 在 $\cup_{N\in\mathbf{N}}U_N=\mathbf{C}$ 上全纯, 即为所证.

(iii) 如果 $\mathrm{Re}(s)>\sigma$, 则 $|\frac{1}{(n^2+1)^s}|\leqslant\frac{1}{(n^2+1)^\sigma}$, 并由于级数 $\sum_{n\in\mathbf{Z}}\frac{1}{(n^2+1)^\sigma}$ 当 $\sigma>\frac{1}{2}$ 时收敛, 由此知级数 $\sum_{n\in\mathbf{Z}}\frac{1}{(n^2+1)^s}$ 在半平面 $\mathrm{Re}(s)>\sigma$ 上按模收敛. 由于每个函数 $s\mapsto\frac{1}{(n^2+1)^s}$ 在 $\mathbf{C}$ 上全纯, 而一个全纯函数的按模收敛的级数也全纯 (定理 V.5.1), 于是 G 在半平面 $\mathrm{Re}(s)>\sigma(\sigma>\frac{1}{2})$ 上全纯, 因而在这些半平面的并上全纯. 得证.

(iv) 如果 $\mathrm{Re}(s)>\frac{1}{2}$, 那么函数 ϕ_s 和它的导数 $t\mapsto\frac{2st}{(1+t^2)^{s+1}}$ 在 $\mathbf{R}$ 上都可和; 因而可将泊松公式应用于它, 又考虑到 $\hat{\phi}_s(n)=\hat{\phi}_s(-n)$, 这便在 $\mathrm{Re}(s)>\frac{1}{2}$ 的情形给出了 [608]

$$G(s)=\hat{\phi}_s(0)+2\sum_{n=1}^{+\infty}F_{1/2}(s,-n).$$

现在, 在右端中的级数也等于 $\hat{\phi}_s(0)+2F(s)$. 由于 F 在整个 $\mathbf{C}$ 上全纯而 G 在半平面 $\mathrm{Re}(s)>\frac{1}{2}$ 上全纯, 故 $\hat{\phi}_s(0)$ 在此半平面上全纯; 因为 $\hat{\phi}_s(0)-\frac{\sqrt{\pi}\Gamma(s-\frac{1}{2})}{\Gamma(s)}$ 在 $]\frac{1}{2},+\infty[$ 上恒等于 0, 故 $\hat{\phi}_s(0)$ 在此半平面与 $\frac{\sqrt{\pi}\Gamma(s-\frac{1}{2})}{\Gamma(s)}$ 重合. 函数 $\frac{\sqrt{\pi}\Gamma(s-\frac{1}{2})}{\Gamma(s)}+2F(s)$ 因此在 $\mathbf{C}$ 上亚纯并除了在 $-k+\frac{1}{2}(k\in\mathbf{N})$ 的单极点外全纯, 并在半平面 $\mathrm{Re}(s)>\frac{1}{2}$ 上等于 $G(s)$; 这就是我们想要的延拓.

(v) 如果 $s=-k,k\in\mathbf{N}$, 那么定义 $G(s)$ 的级数的每一项均为 0 (对于 $\hat{\phi}_s(0)$ 而言, 这是由于 Γ 在负整数上出现的极点, 而对于 $F_{1/2}(s,-n)$, 则是问题 3 的 (iv) 的结果), 因此当 $k\in\mathbf{N}$ 时 $G(-k)=0$.

问题 7. (i) $t\mapsto f(t)^s$ 的 k 阶导数 $f_{s,k}(t)$ 具有 $t\mapsto f(t)^{s-k}P_k(s,f(t),\ldots,f^{(k)}(t))$ 形式, 其中 P_k 是多项式. 特别地, $f_{s,k}(0)$ 具有 $Q_k(s)f(0)^{s-k}$ 形式, 其中 Q_k 是 s 的多项

式. 带积分余项的泰勒公式给出了

$$f(t)^s = \sum_{k=0}^{n} \frac{f(0)^{s-k}Q_k(s)}{k!}t^k + \frac{t^{n+1}}{n!}\int_0^1 f_{s,n+1}(tu)(1-u)^n du.$$

由此得到

$$\int_0^1 t^{as+b}f(t)^s dt = \sum_{k=0}^{n} \frac{f(0)^{s-k}Q_k(s)}{k!(as+b+k+1)} + \int_0^1\int_0^1 t^{as+b+n+1}f_{s,n+1}(tu)(1-u)^n dudt.$$

现在, $s \mapsto g(s,t,u) = t^{as+b+n+1}f_{s,n+1}(tu)(1-u)^n$ 对于 $(t,u) \in [0,1]\times[0,1]$ 在 $\mathrm{Re}(s) > -\frac{b+n+1}{a}$ 上全纯, 并且是 (s,t,u) 的连续函数, 这意味着, 对于 $\mathrm{Re}(s) > -\frac{b+n+1}{a}$ 中的每个紧集 K 存在一个常数 C_K 使得当 $(s,t,u) \in K\times[0,1]^2$ 时, $|g(s,t,u)| \leqslant C_K$. 因此可以利用定理 V.5.7 推出 $s \mapsto \int_0^1\int_0^1 t^{as+b+n+1}f_{s,n+1}(tu)(1-u)^n dudt$ 在半平面 $\mathrm{Re}(s) > -\frac{b+n+1}{a}$ 上全纯. 由于另外的项在整个 $\mathbf{C}$ 上亚纯并且在 $\frac{-b-k}{a}(k \in \{1,\dots,n+1\})$ 有单极点, 故知 $s \mapsto \int_0^1 t^{as+b}f(t)^s dt$ 有到半平面 $\mathrm{Re}(s) > -\frac{b+n+1}{a}$ 上的亚纯延拓, 并在 $\frac{-b-k}{a}(k \in \{1,\dots,n\})$ 上有单极点. 因为这对所有的 $n \in \mathbf{N}$ 为真, 故得结论.

(ii) 将积分 $\int_{-\infty}^{+\infty}$ 分成三段:$]-\infty,-1],[-1,1]$ 和 $[1,+\infty[$, 在 $]-\infty,-1]$ (分别地,$[1,+\infty[$) 上做变量变换 $t = \frac{-1}{u}$ (分别地, $t = \frac{1}{u}$), 则得到 $\int_0^1 u^{ds-2}\frac{1}{(u^dP(-1/u))^s}du$ (分别地, $\int_0^1 u^{ds-2}\frac{1}{(u^dP(1/u))^s}du$), 可以用 (i) 来处理它们. 由于通常的方法可以证明 $s \mapsto \int_{-1}^1 \frac{1}{P(t)^s}dt$ 在整个 $\mathbf{C}$ 上全纯, 故得结论.

(iii) 将 P 写成 $\prod_{j=0}^{d/2}(z-a_j-ib_j)(z-a_j+ib_j)$, 其中所有的 $b_j > 0$. 于是当 $z \in \mathbf{R}$ 时有 $\frac{1}{P(z)^s} = \prod_{j=0}^{d/2}(b_j^{-2s}\phi_s(\frac{z-a_j}{b_j}))$, 由于这个公式定义了 Ω^+ 和 Ω^- 上的一个全纯函数, 从而得到结论 (事实上, 只需去除在半平面 $\mathrm{Im}(z) > 0$ (分别地, $\mathrm{Im}(z) < 0$) 中从 P 的零点出发的竖直半直线即可).

(iv) 如果 $\sigma > \frac{1}{d}$, 则在每个半平面 $\mathrm{Re}(s) > \sigma$ 上这个级数按模收敛, 因此 G_P 在 $\mathrm{Re}(S) > \frac{1}{d}$ 上全纯. 另外, 在此半平面上, $t \mapsto \frac{1}{P(t)^s}$ 及其导数 $t \mapsto \frac{-sP'(t)}{P(t)^{s+1}}$ 可和, 于是可以应用泊松公式, 从而得到 $G_P(s) = \sum_{n\in\mathbf{Z}}\hat{\phi}_{P,s}(n)$. 函数 $s \mapsto \hat{\phi}_{P,s}(0)$ 是 (ii) 中讨论的对象; 它具有到 $\mathbf{C}$ 上的亚纯延拓, 并且除了在 $\frac{1-k}{d}(k \in \mathbf{N})$ 上的单极点外全纯. [609]

问题 5 的 (ii) 的方法可将 $\hat{\phi}_{P,s}(\xi)$ 写成 $e^{-2i\pi\xi z}\phi_{P,s}(z)$ 沿一条道路的积分, 这条道路按照 $\xi < 0$ (分别地, $\xi > 0$), 而由线段 $]-B+i\infty,-B+i\beta],[-B+i\beta,B+i\beta]$ 和 $[B+i\beta,B+i\infty[$ (分别地, $]-B-i\infty,-B-i\beta],[-B-i\beta,B-i\beta]$ 和 $[B-i\beta,B-i\infty[$) 构成, 其中 $B = A+1, \beta \in]0,\alpha[$. 像在问题 3 的 (iii) 那样, 这便证明了 $s \mapsto \hat{\phi}_{P,s}(\xi)$ 可延拓成 $\mathbf{C}$ 上的一个全纯函数, 并且存在一个常数 C_N 使得有 $|\hat{\phi}_{P,s}(\xi)| \leqslant C_N e^{-2\pi\beta|\xi|}$, 其中 $s \in U_N$, 而 ξ 满足 $|\xi| \geqslant 1$. 像在问题 6 的 (ii) 那样, 由此推出 $s \mapsto \sum_{n\in\mathbf{Z}-\{0\}}\hat{\phi}_{P,s}(n)$ 可延拓为 $\mathbf{C}$ 上的一个全纯函数, 从而 G_P 被延拓为 $\mathbf{C}$ 上的一个亚纯函数, 它除了在 $\frac{1-k}{d}(k \in \mathbf{N})$ 上的单极点外全纯.

H.11. 戴德金函数 η

[610]

这节的目标是建立欧拉和雅可比的恒等式[16]

$$q^{1/24}\prod_{n\geqslant 1}(1-q^n)=\sum_{m\in\mathbf{Z}}(-1)^m q^{(6m+1)^2/24}$$

和

$$\sum_{m\in\mathbf{Z}} q^{m^2}w^m=\prod_{n\geqslant 1}(1-q^{2n})(1+q^{2n-1}w)(1+q^{2n-1}w^{-1}).$$

它们是形式恒等式, 但如果令 $q=e^{2i\pi\tau}$, 则它们对于属于庞加莱半平面 $\mathscr{H}=\{z\in\mathbf{C},\mathrm{Im}(z)>0\}$ 的 τ 收敛, 并且我们还将证明, 在 $\mathscr{H}$ 上如此定义的两个函数是相等的. 为得结果我们所遵循的方式[17] 要尽量使用在本教程中所介绍过的技术.

如果 $t\in\mathbf{R}$, 以 Ω_t 记开的半平面 $\{z\in\mathbf{C},\mathrm{Re}(z)>t\}$.

以 $\log:\mathbf{C}^*\to\mathbf{C}$ 为 $-\pi\leqslant\mathrm{Im}(\log z)<-\pi$ 定义的对数分支 (回想一下, $\mathrm{Im}(\log z)$ 也是 z 的幅角 $\arg(z)$). 函数 log 在 $\mathbf{C}-\mathbf{R}_-$ 上全纯, 其导数为 $\frac{1}{z}$, 而函数 $t\mapsto\log(t+i)$ 在 $\mathbf{R}$ 上的导数因此是 $t\mapsto\frac{1}{t+i}$.

如果 $x\in\mathbf{C}^*$ 而 $s\in\mathbf{C}$, 令 $z^s=\exp(s\log z)$, 则有 $|z^s|\leqslant e^{\pi|\mathrm{Im}(s)|}|z|^{\mathrm{Re}(s)}$.

以 Γ 记欧拉 Γ 函数; 它是在 $\mathbf{C}$ 上无处为零的亚纯函数, 在所有 $-n$ 处有单极点, 除此之外处处全纯, 而且对于 $n\in\mathbf{N}$ 有 $\lim_{s\to -n}(s+n)\Gamma(s)=\frac{(-1)^n}{n!}$, 并满足函数方程 $\Gamma(s+1)=s\Gamma(s)$; 实际上, 对于 $s\in\Omega_0$, 它由 $\Gamma(s)=\int_0^{+\infty}e^{-t}t^{s-1}dt$ 给出 (参看定理 VII.2.1).

以 ζ 记黎曼 ζ 函数; 这是一个在 $\mathbf{C}$ 上的亚纯函数, 仅有的一个在 $s=1$ 的单极点外全纯, 并在 Ω_1 上有 $\zeta(s)=\sum_{n=1}^{+\infty}\frac{1}{n^s}$ (参看定理 VII.3.4). 我们有 $\zeta(0)=\frac{-1}{2}$ (习题 VII.3.6).

问题 1. 如果 $s\in\Omega_1$, 定义 $\phi_s:\mathbf{R}\to\mathbf{C}$ 为 $\phi_s(t)=\frac{1}{(t+i)^s}$.

(i) 证明 $\phi_s\in\mathscr{L}^1(\mathbf{R})$ 在 $\mathbf{R}$ 上可微且 $\phi_s'=\frac{-s}{t+i}\phi_s$.

(ii) 证明 $\hat{\phi}_s$ 在无限远速降.

(iii) 证明 $\hat{\phi}_s$ 是微分方程 $xy'+(2\pi x+1-s)y=0$ 的解.

(iv) 由此推出当 $x\leqslant 0$ 时, $\hat{\phi}_s(x)=0$, 并且当 $x>0$ 时, 存在常数 $c(s)$ 使得 $\hat{\phi}_s(x)=c(s)e^{-2\pi x}x^{s-1}$.

问题 2. 设 $s\in\Omega_0$.

(i) 证明当 $\tau\in\Omega_0$ 时 $\int_0^{+\infty}e^{-\tau x}x^{s-1}dx$ 收敛, 并且如此定义的函数 G_s 在 Ω_0(对 τ) 全纯.

---

[16] 当展开这些乘积时它们展示出一些怪异的东西.

[17] 此相等性的组合证明: 参看 Hardy& Wright, *An introduction to the theory of numbers*, §19.11.

(ii) 如果 $\tau \in \mathbf{R}_+^*$, $G_s(\tau)$ 是什么? 由此推出当 $\tau \in \Omega_0$ 时 $G_s(\tau) = \frac{\Gamma(s)}{\tau^s}$.

(iii) 证明 $(1-it)^s = e^{-i\frac{\pi}{2}s}(t+i)^s$, 其中 $t \in \mathbf{R}$.

(iv) 计算 $\hat{\phi}_s$ 的傅里叶反演公式. 由此推出 $c(s) = e^{-\frac{i\pi}{2}s}\frac{(2\pi)^s}{\Gamma(s)}$.

问题 3. (i) 如果 s 是个 $\geqslant 2$ 的整数, 利用留数方法计算 $\hat{\phi}_s$.

(ii) 如果 s 并不是整数, 留数法给出了什么?

[611] **问题 4.** 设 $Y_0 = \{(m,n) \in \mathbf{Z}^2, m > 0, n \geqslant 0\}, Y_1 = \{(m,n) \in \mathbf{Z}^2, m \leqslant 0, n > 0\}$, 又设 $Y = Y_0 \cup Y_1$. (注意这是个不交并且 $\mathbf{Z}^2 - \{(0,0)\}$ 是 Y 和 $-Y = \{-\omega, \omega \in Y\}$ 的不交并.) 设 $\tau \in \mathscr{H}$ 而 $s \in \Omega_2$.

(i) 设 K 为 Ω_2 中的一个紧集. 证明存在 $C(K) > 0$ 和 $a(K) < -2$ 使得对于所有的 $s \in K$ 和 $(m,n) \in Y$ 有 $|\frac{1}{(m+n\tau)^s}| \leqslant C(K)\sup(|m|,|n|)^{a(K)}$.

(ii) 证明级数 $\sum_{(m,n)\in Y}\frac{1}{(m+n\tau)^s}$ 收敛, 并定义了 Ω_2 上的一个全纯函数 $s \mapsto E(\tau, s)$.

(iii) 证明当 $n \geqslant 1$ 时, $\sum_{m\in\mathbf{Z}}\frac{1}{(m+n\tau)^s} = \sum_{\ell=1}^{+\infty} c(s)k^{s-1}e^{2i\pi n\ell\tau}$. (将 $n\tau$ 写成形如 $\alpha + i\beta$ 并关注 $t \mapsto h(t) = \frac{1}{(t+n\tau)^s}$ 的傅里叶变换.)

(iv) 由此推出 $E(\tau,s) = \zeta(s) + e^{-\frac{i\pi}{2}s}\frac{(2\pi)^s}{\Gamma(s)}\sum_{k=1}^{+\infty}\sigma_{s-1}(k)e^{2i\pi k\tau}$, 其中 $\sigma_t(k)$ 代表 k 的因子的 t 次幂的和 (即 $\sigma_t(6) = 1 + 2^t + 3^t + 6^t$). (先证明 $\sum_{d|k}|d^{s-1}| \leqslant k^{\mathrm{Re}(s)}$.)

(v) 证明 $s \mapsto E(\tau,s)$ 有到 $\mathbf{C}$ 的一个亚纯延拓, 并在 $s = 1$ 处的一个单极点外全纯, 而且有 $E(\tau, 0) = -\frac{1}{2}$.

问题 5. 设 φ 是在一个包含半直线 $[0,+\infty[$ 的一个开集上的亚纯函数, 它在 $z = 0$ 上有一个 k 阶极点, 并在此极点外全纯.

(i) 证明存在 $r > 0$ 和 $a_n \in \mathbf{C}$, 使得 $\sum_{n\geqslant -k}|a_n|r^n < +\infty$, 并且当 $|z| \leqslant r$ 时, $\varphi(z) = \sum_{n=-k}^{+\infty}a_n z^n$.

(ii) 证明 $I_1(s) = \int_0^r \varphi(t)t^{s-1}dt$ 当 $\mathrm{Re}(s) > k$ 时收敛, 并具有到整个 $\mathbf{C}$ 的亚纯延拓, 并在 $\leqslant k$ 的整数上的单极点外全纯, 而当 $n \leqslant k$ 时有 $\lim_{s\to n}(s-n)I_1(s) = a_{-n}$. (先证明 $I_1(s) = \sum_{n\geqslant -k}\frac{a_n r^{s+n}}{s+n}$.)

(iii) 进一步假设 φ 在 $+\infty$ 速降. 证明, 当 $\mathrm{Re}(s) > k$ 时, $\Lambda(\varphi, s) = \int_0^{+\infty}\varphi(t)t^{s-1}dt$ 收敛, 并有到 $\mathbf{C}$ 的亚纯延拓, 它在 $\leqslant k$ 的整数上的单极点外全纯, 并满足 $\lim_{s\to n}(s-n)\Lambda(\varphi,s) = a_{-n}$, 其中 $n \leqslant k$.

问题 6. 设 $i = 0, 1$, 而 $f_i(\tau,s) = \sum_{(m,n)\in Y_i}\frac{1}{(m+n\tau)^s}$; 如果 $s \in \Omega_2$, 则有 $E(\tau,s) = f_0(\tau,s) + f_1(\tau,s)$.

(i) 设 $\alpha \in \Omega_0$ 使得 $\alpha\tau \in \Omega_0$. 证明, 当 $(m,n) \in Y_0$ 时, $\frac{1}{(\alpha(m+m\tau))^s} = \frac{1}{\alpha^s(m+n\tau)^s}$.

(ii) 设 $G_\alpha(t) = \frac{1}{(e^{\alpha t}-1)(1-e^{-\alpha\tau t})}$. 证明, 当 $s \in \Omega_2$ 时, $f_0(\tau,s) = \frac{\alpha^s}{\Gamma(s)}\int_0^{+\infty}G_\alpha(t)t^{s-1}dt$. (将问题 2 用于表达式 $\frac{1}{(\alpha(m+n\tau))^s}$.)

(iii) 由此推出 $s \mapsto f_0(\tau,s)$ 具有到整个 $\mathbf{C}$ 的亚纯延拓, 并在单极点 $s = 1$ 和 $s = 2$

外处处全纯.

(iv) 计算 G_α 在 0 的展开式的首项. 由此推出公式[18] $\lim_{s\to 2}(s-2)f_0(\tau,s)=\frac{1}{\tau}, \lim_{s\to 1}(s-1)f_0(\tau,s)=\frac{\tau-1}{2\tau}$ 以及 $f_0(\tau,0)=\frac{\tau}{12}+\frac{1}{12\tau}-\frac{1}{4}$.

问题 7. (i) 在 $(m,n)\mapsto(-n,m)$ 下 Y_0 是什么? 在 $(m,n)\mapsto(n,-m)$ 下 Y_1 又是什么? 由此推出, 如果 k 是个 $\geqslant 2$ 的整数, 则 $E(\frac{-1}{\tau},2k)=\tau^{2k}E(\tau,2k)$.

(ii) 证明 $\log\frac{\tau}{-n+m\tau}=\begin{cases}\log\tau-\log(-n+m\tau), & \text{如果 } (m,n)\in Y_0,\\ \log\tau-\log(n-m\tau)-i\pi, & \text{如果 } (m,n)\in Y_1.\end{cases}$ [612]

(iii) 由此推出, 对于所有 $s\in\mathbf{C}$ 有 $E(\frac{-1}{\tau},s)=\tau^s(E(\tau,s)+(e^{-i\pi s}-1)f_0(\tau,s))$ (先假设 $s\in\Omega_2$.)

(iv) 证明 $E(\frac{-1}{\tau},2)=\tau^2E(\tau,2)-i\pi\tau$.

问题 8. 以 $F(\tau)$ 记 $s\mapsto E(\tau,s)$ 在 $s=0$ 的导数.

(i) 证明乘积 $e^{i\pi\tau/12}\prod_{n=1}^{+\infty}(1-e^{2i\pi n\tau})$ 对 $\tau\in\mathscr{H}$ 收敛, 并且如此定义的函数 $\eta:\mathscr{H}\to\mathbf{C}$ 在 $\mathscr{H}$ 上全纯并不取零值.

(ii) 证明存在一个在 $\mathscr{H}$ 上全纯并满足 $e^g=\eta$ 的函数 g, 并且存在 $a\in\mathbf{Z}$ 使得 $g=h+a2i\pi$, 其中对于 $\tau\in\mathscr{H}$ 有 $h(\tau)=\frac{i\pi\tau}{12}+\sum_{n=1}^{+\infty}\log(1-e^{2i\pi n\tau})$. (以 $\log\eta$ 记函数 h.)

(iii) 证明存在 $C\in\mathbf{C}$ 使得对于所有 $\tau\in\mathscr{H}$ 有 $\log\eta(\tau)=-F(\tau)+\frac{i\pi\tau}{12}+C$.

(iv) 由此推出 $\log\eta(\frac{-1}{\tau})=\frac{1}{2}\log\tau+\log\eta(\tau)-\frac{i\pi}{4}$ 和 $\eta(\frac{-1}{\tau})=\sqrt{\frac{\tau}{i}}\eta(\tau)$, 其中 $\tau\in\mathscr{H}$, 而 $\sqrt{\frac{\tau}{i}}$ 是在 $\tau=i$ 取 1 的分支.

(v) 利用 (iii) 的恒等式证明 $\frac{\eta'(\tau)}{\eta(\tau)}+\frac{1}{2i\pi}E(\tau,2)=0$; 由此推出 $\zeta(2)=\frac{\pi^2}{6}$.

问题 9. 如果 $\tau\in\mathscr{H}$, 则级数 $\sum_{m\in\mathbf{Z}}(-1)^m e^{2i\pi\frac{(6m+1)^2\tau}{24}}$ 收敛, 从而如此定义的函数 $\tau\mapsto H(r)$ 由通常的理由得知其在 $\mathscr{H}$ 上全纯. 我们让读者自己去解决该如何相信也成立 $H(\tau)=\frac{1}{2}\sum_{n\in\mathbf{Z}}\chi(n)e^{2i\pi\frac{n^2\tau}{24}}$, 其在 $\chi:(\mathbf{Z}/12\mathbf{Z})^*\to\{\pm1\}$ 是一个狄利克雷特征标, 它的定义是 $\chi(1)=\chi(-1)=1$ 而 $\chi(5)=\chi(-5)=-1$, 我们可将它看作是从 $\mathbf{Z}$ 到 $\{\pm1\}$ 的周期为 12 的周期函数, 其在与 12 非互素的整数 (即被 2, 3 整除的整数) 上取 0.

(i) 回顾: 已知 $t\mapsto e^{-\pi t^2}$ 的傅里叶变换是 $x\mapsto e^{-\pi x^2}$. 计算当 $y>0, a\in\mathbf{Z}$ 时的 $t\mapsto e^{-2i\pi\frac{at}{12}}e^{-\pi\frac{yt^2}{12}}$ 的傅里叶变换. 由此推出恒等式

$$\sum_{n\in\mathbf{Z}}e^{-2i\pi\frac{an}{12}}e^{-\pi\frac{yn^2}{12}}=\sqrt{\frac{12}{y}}\sum_{n\in\mathbf{Z}}e^{-\frac{\pi}{12y}(12n+a)^2}.$$

[18] 同样的方法可推出公式 $f_1(\tau,s)=\frac{\alpha^s}{\Gamma(s)}\int_0^{+\infty}\frac{1}{(e^{\alpha t}-1)(1-e^{\alpha\tau t})}t^{s-1}dt$, 其中 α 满足 $\mathrm{Re}(\alpha\tau)>0$ 和 $\mathrm{Re}(-\alpha)>0$, 于是可以证明 $f_1(\tau,s)$ 也具有到整个 $\mathbf{C}$ 的亚纯延拓, 并且在 $s=2$ 的单极点 (留数为 $-\frac{1}{\tau}$) 和在 $s=1$ 的单极点 (留数为 $\frac{1+\tau}{2\tau}$) 之外全纯, 而且重新证明了问题 4 以及在前言中回顾的那些 ζ 的性质.

(ii) 证明[19] 对所有 $n \in \mathbf{Z}$ 有 $\frac{1}{\sqrt{12}} \sum_{a=-5}^{6} \chi(a) e^{-2i\pi \frac{an}{12}} = \chi(n)$.

(iii) 推导对于 $\tau \in \mathscr{H}$ 有 $H(\frac{-1}{\tau}) = \sqrt{\frac{\tau}{i}} H(\tau)$. (先从 $\tau \in i\mathbf{R}_+^*$ 着手.)

(iv) 证明 $J(\tau) = H(\tau)/\eta(\tau)$ 是 $\mathscr{H}$ 上的全纯函数, 且对于所有的 $\tau \in \mathscr{H}$ 满足函数方程 $J(\tau+1) = J(\tau)$ 和 $J(\frac{-1}{\tau}) = J(\tau)$[20].

(v) 证明存在在 $D(0,1^-)$ 上唯一的全纯函数 $q \mapsto \tilde{J}(q)$ 使得对所有的 $\tau \in \mathscr{H}$ 有 $J(\tau) = \tilde{J}(e^{2i\pi\tau})$. $J(0)$ 是什么?

(vi) 设 $X = \{\tau = x + iy, |x| < \frac{2}{3}, y > \frac{1}{3}\}$. 以 ∂X 为开集 X 的边界 (由竖直半直线 $[\frac{-2+i}{3}, \frac{-2}{3} + i\infty[$, $[\frac{2+i}{3}, \frac{2}{3} + i\infty[$ 和水平线段 $[\frac{-2+i}{3}, \frac{2+i}{3}]$ 组成), 并设 $\overline{X} = X \cup \partial X$ 为 X 的闭包. 证明存在 $c > 0$ 使得对所有的 $\tau = x + iy \in \overline{X}$ 有 $|J(\tau) - 1| \leqslant ce^{-2\pi y}$. 由此推出 $|J-1|$ 在 ∂X 上达到它在 $\overline{X}$ 中的最大值.

[613] (vii) 设 $\tau \in \partial X$. 证明至少 5 个数 $\tau+1, \tau-1, \frac{-1}{\tau}, \frac{-1}{\tau}+1, \frac{-1}{\tau}-1$ 有一个属于 X. 由此推出 J 为常值, 从而 $H = \eta$[21].

问题 10. (i) 证明如果 $|q| < 1$, 则对于 $w \in \mathbf{C}^*$, 乘积 $\prod_{n \geqslant 1} (1 - q^{2n})(1 + q^{2n-1}w)(1 + q^{2n-1}w^{-1})$ 收敛, 并且如此定义的函数 $w \mapsto A(q,n)$ 在 $\mathbf{C}^*$ 上全纯.

(ii) 由此得到, 存在唯一的定义在 $D(0,1^-)$ 上对所有 $m \in \mathbf{Z}$ 的 a_m, 使得对所有 $w \in \mathbf{C}^*$ 及 $q \in D(0,1^{-1})$, 有 $A(q,w) = \sum_{m \in \mathbf{Z}} a_m(q) w^m$.

(iii) 证明对所有的 $w \in \mathbf{C}^*$ 及 $q \in D(0,1^-)$ 有 $A(q, q^2 w) = q^{-1} w^{-1} A(q,w)$.

(iv) 由此推出对所有 $m \in \mathbf{Z}$ 成立 $a_m(q) = q^{m^2} a_0(q)$.

(v) 以两种方式计算 $A(e^{3i\pi\tau}, -e^{i\pi\tau})$, 其中 $\tau \in \mathscr{H}$; 由此得到雅可比三重乘积公式:

$$\sum_{m \in \mathbf{Z}} q^{m^2} w^m = \prod_{n \geqslant 1} (1 - q^{2n})(1 + q^{2n-1}w)(1 + q^{2n-1}w^{-1}).$$

(vi) 在 $\mathscr{H}$ 上的雅可比 θ 函数的定义是 $\theta(\tau) = \sum_{m \in \mathbf{Z}} e^{i\pi m^2 \tau}$. 证明, 对于 $\tau \in \mathscr{H}$ 有 $\theta(\tau) = \frac{\eta(\tau)^5}{\eta(2\tau)^2 \eta(\tau/2)^2}$.

---

[19] 这是引理 VII.4.3 的特殊情形.

[20] 换言之, J 是一个权为 0 的模形式 (参考 VII.6).

[21] 问题 7 的函数 $E_{2k} = E(\tau, 2k) = \zeta(2k) + (-1)^k \frac{(2\pi)^{2k}}{(2k-1)!} \sum_{n \geqslant 1} \sigma_{2k-1}(n) q^n$ 是称作艾森斯坦级数的模形式; 函数 η 是所谓的戴德金 η 函数; 而它的 24 次幂 $\Delta = q \prod_{n \geqslant 1} (1 - q^n)^{24}$ 则是模形式论中的一个罗曼蒂克对象; 拉马努金有许多关于它的工作. 我们可以以同样的方法证明 $\zeta(6)^2 E_4^3 - \zeta(4)^3 E_6^2 = \alpha\Delta$, 其中 $\alpha = 3\frac{(2\pi)^4}{3!} \zeta(6)^2 \zeta(4)^2 + 2\frac{(2\pi)^6}{5!} \zeta(4)^3 \zeta(6)$ 或者 $\zeta(8) E_4^2 = \zeta(4)^2 E_8$ (考虑 $\Delta^{-2}(\zeta(8)E_4^2 - \zeta(4)^2 E_8)^3$) 或者还可证明 E_{2k} 是 E_4 和 E_6 的多项式.

η 函数出现在许多不同的场合, 例如, 我们将方程 $y^2 + y = x^3 - x^2$ 在 $\mathbf{F}_p$ 中的解的个数写成 $p + a_p$ 形式, 并构造乘积 $\frac{1}{1-11^{-s}} \prod_{p \neq 11} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$, 并将它展开为 $\sum_{n \geqslant 1} a_n n^{-s}$ 形式. 于是, $\sum_{n \geqslant 1} a_n q^n = \eta(\tau)^2 \eta(11\tau)^2$ (Eichler, 1954). 这个结果催生了一个著名的猜想 (谷山 – 韦伊猜想), 而这个猜想则与椭圆曲线和模形式相关, 它的一个部分结果让怀尔斯得以证明费马大定理; 一般情形也已由 Breuil, Conrad, Diamond 和 Taylor 证明 (1999).

问题校正

问题 1. (i) 我们有 $|\phi_s(t)| \leqslant e^{\pi \mathrm{Im}(s)}(1+t^2)^{-\mathrm{Re}(s)/2}$, 因此在 $\pm\infty$ 的邻域中 $\phi_s(t) = O(|t|^{-\mathrm{Re}(s)})$, 这证明了 ϕ_s 可和, 而由于 $t \mapsto \log(t+i)$ 连续, 故函数 ϕ_s 在 $\mathbf{R}$ 上连续. 另外, $t \mapsto \log(t+i)$ 可微且导数为 $\frac{1}{t+i}$, 这表明 $\phi_s = \exp(-s\log(t+i))$ 可微, 其导数为 $t \mapsto -s\frac{1}{t+i}\exp(s\log(t+i)) = \frac{-s}{t+i}\phi_s$, 即为所求.

(ii) 从 (i) 得知 ϕ_s 属于 $\mathscr{C}^k$, 其中 k 任意, 且 $\phi_s^{(k)} = (-s)(-s-1)\cdots(-s-k+1)\phi_{s+k}$ 对所有的 k 可和. 因此按照定理 IV.2.8 有 $(1+x^2)^{k/2}|\hat{\phi}_s(x)|$ 对于所有 $k \in \mathbf{N}$ 在无限远趋向 0, 从而 $\hat{\phi}_s$ 在无限远速降.

(iii) 以 y 记 ϕ_s 的傅里叶变换, 由定理 IV.2.8 的 (i) 和问题的 (ii) 知 ϕ_s' 的傅里叶变换是 $2i\pi xy$, 并由定理 IV.2.8 的 (ii) 得知 $t \mapsto t\phi_s'$ 的傅里叶变换是 $x \mapsto \frac{-1}{2i\pi}(2i\pi xy)' = -xy' - y$. 将 $\mathscr{F}$ 作用于恒等式 $t\phi_s' + i\phi_s' + s\phi_s = 0$ 便给出了关系式 $-xy' - y - 2\pi xy + sy = 0$ 或者 $xy' + (2\pi x + 1 - s)y = 0$, 即为所求.

(iv) 上面的微分方程可重写为 $\frac{y'}{y} = -2\pi + \frac{s-1}{x}$, 其在 $\mathbf{R}_+^*$ 和 $\mathbf{R}_-^*$ 上的解具有 $c^{\pm}e^{-2\pi x}|x|^{s-1}$ 形式. 然而已知 $\hat{\phi}_s$ 在无限远速降, 这表明 $c^- = 0$. 由此得结果. [614]

问题 2. (i) 如果 $a > 0$, 则对于所有的 $x \in \mathbf{R}_+$ 和 $\tau \in \Omega_a$ 有 $|e^{-\tau x}x^{s-1}| \leqslant e^{-ax}x^{s-1}$, 并由于 $x \mapsto e^{-ax}x^{s-1}$ 在 $\mathbf{R}_+$ 上可和, 而对所有 $x \in \mathbf{R}_+$, $\tau \mapsto e^{-\tau x}x^{s-1}$ 在 Ω_a 上全纯, 于是我们可以应用定理 V.5.7 推出 $\tau \mapsto G_s(\tau) = \int_0^{+\infty} e^{-\tau x}x^{s-1}dx$ 在 Ω_a 上全纯. 因为它对每个 $a > 0$ 都成立, 故 G_s 在 $\cup_{a>0}\Omega_a = \Omega_0$ 上全纯.

(ii) 如果 $\tau \in \mathbf{R}_+^*$, 则通过变量变换 $x = \frac{u}{\tau}$ 得到 $G_s(\tau) = \int_0^{+\infty} e^{-u}u^{s-1}\tau^{1-s}\frac{du}{\tau} = \frac{\Gamma(s)}{\tau^s}$. 现在, $\tau \mapsto \frac{\Gamma(s)}{\tau^s}$ 在 Ω_0 上全纯, 因此 $G_s(\tau) - \frac{\Gamma(s)}{\tau^s}$ 在连通开集 Ω_0 上全纯, 并在 $\mathbf{R}_+^*$ 上为 0. 于是根据孤立零点定理它恒等于 0. 得到结论.

(iii) 如果 $t \in \mathbf{R}$, 则有 $\mathrm{Im}(\log(t+i)) \in]0,\pi[$, 由此得到 $\mathrm{Im}(\log(t+i) - \frac{i\pi}{2}) \in]-\frac{\pi}{2}, \frac{\pi}{2}[\subset [-\pi,\pi[$, 因此 $\log(1-it) = \log\frac{t+i}{i} = \log(t+i) - \frac{i\pi}{2}$, 即为所求.

(iv) 由于 $\hat{\phi}_s$ 在无限远速降并连续, 故可和, 那么从 L^1 中的傅里叶反演公式 (命题 IV.3.25) 得到 $\overline{\mathscr{F}}\hat{\phi}_s = \phi_s$. 另外, 我们有

$$\overline{\mathscr{F}}\hat{\phi}_s(t) = \int_{-\infty}^{+\infty} e^{2i\pi tx}\hat{\phi}_s(x) = c(s)\int_0^{+\infty} e^{2i\pi tx}e^{-2\pi x}x^{s-1}dx,$$

于是 (ii) 和 (iii) 给出了 $\overline{\mathscr{F}}\hat{\phi}_s(t) = \frac{c(s)\Gamma(s)}{(2\pi(1-it))^s} = \frac{c(s)e^{i\frac{\pi}{2}s}\Gamma(s)}{(2\pi)^s}\phi_s(t)$. 由此推出了结果.

问题 3. (i) 如果 $x > 0$, 我们对函数 $g_s(z) = \frac{e^{-2i\pi zx}}{(z+i)^s}$ 沿道路 γ_R 积分, 其中的道路由线段 $[-R,R]$ 和中心在 0 半径为 R 的下半圆组成. 函数 g 在 $\mathbf{C}$ 上亚纯, 并在 $z = -i$ 的极点外全纯, 而在此点的留数 $\mathrm{Res}(g_s,-i)$ 是 $e^{-2i\pi zx}$ 的泰勒展开式中的 $s-1$ 次项, 即 $\frac{1}{(s-1)!}(-2i\pi x)^{s-1}e^{-2i\pi(-i)x} = (-i)^{s-1}\frac{(2\pi)^{s-1}}{(s-1)!}e^{-2\pi x}$. 当 $R > 1$ 时, 我们有 $I(\gamma_R,-i) = -1$, 因此 $\int_{\gamma_R} g_s(z)dz = -2i\pi(-i)^{s-1}\frac{(2\pi)^{s-1}}{(s-1)!}e^{-2\pi x} = (-i)^s\frac{(2\pi)^s}{\Gamma(s)}e^{-2\pi x}$.

当 $R \to +\infty$ 时, 在线段上的这个积分趋向 $\hat{\phi}_s(x)$, 而在此半圆上我们有囿

于上的不等式 $|e^{-2i\pi zx}| \leqslant 1$ 和 $|\frac{1}{(z+i)^s}| \leqslant \frac{1}{(R-1)^s}$. 而由于此半圆弧的长为 πR, 故在此半圆弧上的积分按模被 $\frac{\pi R}{(R-1)^s}$ 囿于上; 因而它趋向 0. 取极限于是给出 $\hat{\phi}_s(x) = (-i)^s \frac{(2\pi)^s}{\Gamma(s)} e^{-2\pi x}$, 这与问题 2 的结果相匹配.

如果 $x \leqslant 0$, 我们则沿 γ_R^+ 对 $g_s(z)$ 积分, 其中 γ_R^+ 由线段 $[-R, R]$ 和中心在 0 半径为 R 的上半圆弧组成. 与前面的计算唯一不同之处是 $I(\gamma_R^+, -i) = 0$, 因此沿此道路的积分为 0, 这给出了 $\hat{\phi}_s(x) = 0$.

(ii) 如果 s 不是整数, 因为 g_s 在包含 γ_R^+ 的一个开集中全纯, 则如上面那样, 留数法可证明当 $x \leqslant 0$ 时 $\hat{\phi}_s(x) = 0$. 相反地, 因为 g_s 不在包含 γ_R 的开集上亚纯, 故不能通过计算留数来计算 $\hat{\phi}_s$(沿从 $-i$ 出发的半直线有一个间断点, 并依赖于 log 分支的选取[22]).

[615] **问题 4.** (i) 范数 $|x+\tau y|$ 和 $\sup(|x|, |y|)$ 在 $\mathbf{R}^2$ 上是等价的; 故存在 $c > 0$ 使得对所有的 $(x,y) \in \mathbf{R}^2$ 有 $|x+\tau y| \geqslant c \sup(|x|, |y|)$. 因此有 $|\frac{1}{(m+\tau n)^s}| \leqslant e^{-\mathrm{Re}(s)} e^{\pi|\mathrm{Im}(-s)|} \frac{1}{\sup(|m|,|n|)^{\mathrm{Re}(s)}}$. 由此得到了这个结果, 其中 $a(K) = -\inf_{s\in K} \mathrm{Re}(s)$ (因为这个 inf 在紧集 K 的一个点达到, 故有 $a(K) < -2$) 并且 $C(K) = \sup_{s\in K} c^{\mathrm{Re}(s)} e^{\pi|\mathrm{Im}(-s)|}$ (因为这个 sup 在此紧集上的一点达到, 故有 $C(K) < +\infty$).

(ii) 如果 $k \in \mathbf{N} - \{0\}$, 则有 $(2k+1)^2 - (2k-1)^2 = 8k$ 个偶对 $(m, n) \in \mathbf{Z}^2$, 它满足 $\sup(|m|, |n|) = k$, 从而 $4k \in Y$. 如果 K 是 Ω_2 中的一个紧集, 则由于 $1 + a(K) < -1$, 便有 $\sum_{(m,n)\in Y} |\frac{1}{(m+n\tau)^s}| \leqslant \sum_{k=1}^{+\infty} 4kC(K)k^{a(K)} < +\infty$. 这个级数因此在 Ω_2 中的任意紧集上按范数收敛, 因为其中的每一项 $s \mapsto \frac{1}{(m+n\tau)^s}$ 显然是全纯的, 所以可以利用定理 V.5.1 证明它的和在 Ω_2 上全纯.

(iii) 函数 h 和它的导数都可和. 因此可利用泊松公式 (定理 IV.3.11) 得到 $\sum_{m\in\mathbf{Z}} h(m) = \sum_{\ell\in\mathbf{Z}} \hat{h}(\ell)$. 我们有 $\hat{h}(x) = \int_{\mathbf{R}} e^{-2i\pi tx} \frac{1}{(t+\alpha+i\beta)^s} dt$. 变量变换 $t = \alpha u - \beta$ 使得

$$\hat{h}(x) = \beta^{1-s} e^{2i\pi\alpha x} \hat{\phi}_s(\beta x) = \beta^{1-s} e^{2i\pi\alpha x} c(s) e^{-2\pi\beta x} (\beta x)^{s-1} = c(s) x^{s-1} e^{2i\pi n\tau x}.$$

由此得到结果.

---

[22]可以选择切断竖直直线 $[-i, -i\infty[$, 并在由中心在 0 半径为 R 的 (几乎) 四分之一的圆周, 线段 $[-iR+\varepsilon, -i-\varepsilon]$, 中心在 $-i$ 半径为 ε 的以逆时针方向为正向的半圆, 线段 $[-i-\varepsilon, -iR-\varepsilon]$ 以及中心在 0 半径为 R 的另一个 (几乎) 四分之一的圆周 (请作图) 组成的道路上积分. 由于可以在一个点上对道路形变并保持在此半直线的补集中, 故 g_s 在此闭道上的积分为 0. 另外, 当 R 和 ε 趋向 $+\infty$ 和 0 时, 在 $[-R, R]$ 上的积分趋向 $\hat{\phi}_s(x)$, 而沿竖直线段上的积分趋向在半直线 $[-i\infty, -i[$ 上的积分 (应该注意到对数的值在出现的这两条半直线上的值是不一样的). 做变量变换 $t = -i(1+u)$, 由此得到在从 $-i\infty$ 到 $-i$ 和从 $-i$ 到 $-i\infty$ 的两条半直线上

$$\begin{aligned}\int_{-\infty}^{+\infty} \frac{1}{(t+i)^s} e^{-2i\pi tx} dt &= i(e^{-\frac{3i\pi}{2}s} - e^{\frac{i\pi}{2}s}) e^{-2\pi x} \int_0^{+\infty} e^{-2\pi xu} u^{-s} du \\ &= 2e^{-\frac{i\pi}{2}s} \sin\pi s \Gamma(1-s) \frac{e^{-2\pi x}}{(2\pi x)^{1-s}}.\end{aligned}$$

与问题 2 的比较便给出了互补公式 $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin\pi s}$.

(iv) 结果通过变量变换 $d=n, k=\ell n$ 将和 $\sum_{n=1}^{+\infty}\sum_{\ell=1}^{+\infty}$ 变换为 $\sum_{k=1}^{+\infty}\sum_{d|k}$ 得到. 然而还应该证明随意重新安排项的合理性; 为此它涉及要证明这个二重级数是绝对收敛的, 即当 $\sigma=\mathrm{Re}(s)>2$ 和 $\alpha=\mathrm{Im}(\tau)>0$ 时 $\sum_{n=1}^{+\infty}\sum_{l=1}^{+\infty}\ell^{\sigma-1}e^{-2\pi\alpha n\ell}<+\infty$. 但我们可以在这个正项级数中利用上面的变量变换得到 $\sum_{k=1}^{+\infty}\sum_{d|k}d^{\sigma-1}e^{-2\pi\alpha k}$, 并由于 k 最多只有 k 个因子, 故此和 $\leqslant k$, 于是它被 $\sum_{k=1}^{+\infty}k^{\sigma}e^{-2\pi\alpha k}$ 囿于上, 这个和是有限的. 得到结论.

(v) $s\mapsto\sum_{k=1}^{+\infty}\sigma_{s-1}(k)e^{2i\pi k\tau}$ 是一个全纯函数的级数, 它在所有形如 $\mathrm{Re}(s)\leqslant a(a\geqslant 1)$ 的半平面上按范数收敛 (在这样的半平面上我们有 $|\sigma_{s-1}(k)|\leqslant k^a$). 现在可以利用在前言中所回顾的 ζ 函数和 Γ 函数的性质来得出结论 (特别地, 我们得到 $s\mapsto e^{-i\frac{\pi}{2}s}\frac{(2\pi)^s}{\Gamma(s)}$ 在 $\mathbf{C}$ 上全纯, 并且 $s=-n(n\in\mathbf{N})$ 为零点.)

由于 $\frac{1}{\Gamma}$ 在 $s=0$ 为 0, 故有 $E(\tau,0)=\zeta(0)=\frac{-1}{2}$.

问题 5. (i) 设 Ω 是一个包含 $[0,+\infty[$ 的开集, 在其上 φ 在唯一的在 0 的极点外全纯. 因此我们有 $\varphi(z)=\sum_{i=1}^{k}\frac{a_{-i}}{z^i}+u(z)$, 其中 u 在 Ω 上全纯. 令 $r_1=d(0,\mathbf{C}-\Omega)$. 于是 u 是在 $D(0,r_1^-)$ 上它的泰勒级数的和 (参看注记 V.4.9 的 (i)), 且它在所有闭集 $D(0,r)(r<r_1)$ 上收敛, 从而绝对收敛. 对于这样的 r. 我们可在 $|z|\leqslant r$ 上将 $\varphi(z)$ 写成 $\sum_{n\geqslant -k}a_nz^n$, 并且 $\sum_{n\geqslant -k}|a_n|r^n<+\infty$.

(ii) 我们有 $t^{s-1}\varphi(t)=\sum_{n=-k}^{+\infty}a_nt^{s+n-1}$. 但是如果 $\mathrm{Re}(s)>k$, 且因为当 $n\neq -k$ 时 $\mathrm{Re}(s+n)\geqslant 1$ 以及 $\sum_{n=-k}|a_n|r^{\mathrm{Re}(s)+n}<+\infty$, 故 $\sum_{n=-k}^{+\infty}\int_0^r|a_nt^{s+n-1}|dt\leqslant\sum_{n=-k}^{+\infty}\frac{|a_n|r^{\mathrm{Re}(s)+n}}{\mathrm{Re}(s+n)}<+\infty$. 由在 $\mathbf{N}\times X$ 上的富比尼定理得到此级数在 $L^1([0,r])$ 上收敛 (因此此级数和可和), 并得知此和与积分可以交换, 这便给出了 $I_1(s)=\sum_{n\geqslant -k}\frac{a_nr^{s+n}}{s+n}$.

设 $N\geqslant k$. 我们将这个级数分割为 $\sum_{n=-k}^{N}\frac{a_nr^{s+n}}{s+n}$ 和 $\sum_{n\geqslant N+1}\frac{a_nr^{s+n}}{s+n}$ 两部分; 前者是 $\mathbf{C}$ 上的一个亚纯函数, 它在满足 $-N\leqslant n\leqslant k$ 的 $n\in\mathbf{Z}$ 上为单极点, 其留数为 a_{-n}; 而后者由于当 $n\geqslant N+1, |s|<N$ 时有 $|\frac{a_nr^{s+n}}{s+n}|\leqslant r^{\mathrm{Re}(s)}|a_nr^n|$, 故它在 $D(0,N^-)$ 上按范数收敛. 由此并根据定理 V.5.1 知, $\sum_{n\geqslant N+1}\frac{a_nr^{s+n}}{s+n}$ 在 $D(0,N^-)$ 上定义了一个全纯函数, 因而 I_1 在 $D(0,N^-)$ 上亚纯, 并在满足 $-N\leqslant n\leqslant k$ 的 $n\in\mathbf{Z}$ 上具有留数为 a_{-n} 的单极点, 除此之外全纯. 所求的结果由将 $\mathbf{C}$ 写成 $D(0,N^-)(N\in\mathbf{N})$ 的并而得到. [616]

(iii) 分解 $\Lambda(\varphi,s)$ 为 $I_1(s)+I_2(s)$, 其中 $I_1(s)=\int_0^r\varphi(t)t^{s-1}dt$ 和 $I_2(s)=\int_r^{+\infty}\varphi(t)t^{s-1}dt$. 函数 $s\mapsto I_1(s)$ 在 (ii) 中已经研究过; 因此只需研究 $s\mapsto I_2(s)$. 如果 φ 在无限远速降, 那么 $\int_r^{+\infty}\varphi(t)t^{s-1}dt$ 对于每个 $s\in\mathbf{C}$ 收敛. 在一个竖直带 $a<\mathrm{Re}(s)<b$ 上 $|t^{s-1}\varphi(t)|$ 被 $\sup(t^a,t^b)|\varphi(t)|$ 囿于上, 故在 $[r,+\infty[$ 上可和. 由此并利用定理 V.5.7 得知 $s\mapsto I_2(s)$ 在此带上全纯, 并由于 $\mathbf{C}$ 是这些带的并, 这证明了 $s\mapsto I_2(s)$ 在 $\mathbf{C}$ 上全纯. 得到结果.

问题 6. (i) 条件 $\mathrm{Re}(\alpha)>0$ 和 $\mathrm{Re}(\alpha\tau)>0$ 可化为 $0<\arg(\alpha)<\pi-\arg(\tau)$. 另外, 如

果 $(m,n)\in Y_0$, 则有 $0\leqslant \arg(m+n\tau)\leqslant \arg(\tau)$, 从而 $0\leqslant \arg(\alpha)+\arg(m+n\tau)<\pi$, 我们推断 $\arg(\alpha(m+n\tau))=\arg(\alpha)+\arg(m+n\tau)$, 故有结论.

(ii) 根据问题 2, 如果 $\omega\in Y_0$, 则有 $\frac{1}{(\alpha\omega)^s}=\frac{1}{\Gamma(s)}\int_0^{+\infty}e^{-t\alpha\omega}t^{s-1}dt$. 由此推出 $f_0(\tau,s)=\frac{\alpha^s}{\Gamma(s)}\sum_{\omega\in Y_0}\int_0^{+\infty}e^{-t\alpha\omega}t^{s-1}dt$. 我们有

$$\begin{aligned}\sum_{\omega\in Y_0}|e^{-t\alpha\omega}t^{s-1}| &= t^{\sigma-1}\sum_{m=1}^{+\infty}\sum_{n=0}^{+\infty}e^{-t(n\mathrm{Re}(\alpha)+m\mathrm{Re}(\alpha\tau))}\\ &= \frac{t^{\sigma-1}}{(e^{t\mathrm{Re}(\alpha)}-1)(1-e^{-t\mathrm{Re}(\alpha\tau)})},\end{aligned}$$

由于它在无限远速降且在 0 的邻域上 (且 $\sigma-3>-1$) 为 $O(t^{\sigma-3})$. 因此我们可以交换取和与积分, 而以上面同样的计算证明了 $\sum_{\omega\in Y_0}e^{-t\alpha\omega}=G_\alpha(t)$, 故得结论.

(iii) 函数 $G_\alpha(t)$ 满足问题 5(iii) 的条件. 由此得知 $\Gamma(s)\alpha^{-s}f_0(\tau,s)$ 具有到 $\mathbf{C}$ 的亚纯延拓, 其在 $\leqslant 2$ 的整数上有单极点. 由于 $\frac{1}{\Gamma(s)}$ 在 $\mathbf{C}$ 上全纯, 其在负整数上具有单零点, 这意味着 $f_0(\tau,s)$ 在 $s=1$ 和 $s=2$ 的单极点外全纯.

(iv) 我们有

$$\begin{aligned}G_\alpha(z) &= \frac{1}{(e^{\alpha z}-1)(1-e^{-\alpha\tau z})}\\ &= \frac{1}{\alpha^2\tau z^2}\frac{1}{(1+\frac{\alpha z}{2}+\frac{\alpha^2z^2}{6}+\cdots)(1-\frac{\alpha\tau z}{2}+\frac{\alpha^2\tau^2z^2}{6}+\cdots)}\\ &= \frac{1}{\alpha^2\tau z^2}+\frac{1}{\alpha z}\frac{\tau-1}{2\tau}+\frac{1}{12\tau}+\frac{\tau}{12}-\frac{1}{4}+\cdots.\end{aligned}$$

现在, 按照 (ii), $\lim_{s\to n}(s-n)\Gamma(s)\alpha^{-s}f_0(\tau,s)$ 是 G_α 在 0 的邻域中的洛朗展开式的 $-n$ 次的系数. 由此得到 $\alpha^{-2}\lim_{s\to 2}(s-2)f_0(\tau,s)=\frac{1}{\alpha^2\tau}$, 因此 $\lim_{s\to 2}(s-2)f_0(\tau,s)=\frac{1}{\tau}$. 同样, $\alpha^{-1}\lim_{s\to 1}(s-1)f_0(\tau,s)=\frac{\tau-1}{2\alpha\tau}$, 从而 $\lim_{s\to 1}(s-1)f_0(\tau,s)=\frac{\tau-1}{2\tau}$. 最后, 由于 $\lim_{s\to 0}\alpha^{-s}s\Gamma(s)=1$, 故有 $f_0(\tau,0)=\frac{1}{12\tau}+\frac{\tau}{12}-\frac{1}{4}$.

问题 7. (i) $(m,n)\mapsto(-n,m)$ 诱导了从 Y_0 到 Y_1 的双射, 而 $(m,n)\mapsto(n,-m)$ 则诱导了从 Y_1 到 Y_0 的双射.

现在, $E(\frac{-1}{\tau},2k)=\sum_{(m,n)\in Y}(m+\frac{-n}{\tau})^{-2k}=\tau^k\sum_{(m,n)\in Y}\frac{1}{(-n+m\tau)^{2k}}$. 由于这个级数绝对收敛, 则可以将这些项按照任意的次序取和, 并由于 $(-n+m\tau)^{2k}=(n-m\tau)^{2k}$, 于是有 $E(\frac{-1}{\tau},2k)=\sum_{(m,n)\in Y_0}\frac{1}{(-n+m\tau)^{2k}}+\sum_{(m,n)\in Y_1}\frac{1}{(n-m\tau)^{2k}}$. 然而, $(m,n)\mapsto(-n,m)$ 诱导了从 Y_0 到 Y_1 的双射, 故而第一个和等于 $\sum_{(m,n)\in Y_1}\frac{1}{(m+n\tau)^{2k}}$, 同时因为 $(m,n)\mapsto(n,-m)$ 诱导了从 Y_1 到 Y_0 的一个双射, 故第二个和等于 [617] $\sum_{(m,n)\in Y_0}\frac{1}{(m+n\tau)^{2k}}$. 于是得到结论.

(ii) 我们有 $0<\arg(\tau)<\pi$.

如果 $(m,n)\in Y_0$, 则 $0\leqslant\arg(-n+m\tau)<\pi$, 从而 $-\pi<\arg(\tau)-\arg(-n+m\tau)<\pi$, 这表明 $\arg(\frac{\tau}{-n+m\tau})=\arg(\tau)-\arg(-n+m\tau)$. 于是得到在这种情形下的结论.

如果 $(m,n)\in Y_1$, 则有 $0\leqslant \arg(n-m\tau)<\arg(\tau)$, 因而有 $0<\arg(\frac{\tau}{n-m\tau})=\arg(\tau)-\arg(n-m\tau)<\pi$. 由此得到 $\arg(\frac{\tau}{-n+m\tau})=\arg(\frac{\tau}{n-m\tau})-\pi$. 得到结论.

(iii) 先假设 $\mathrm{Re}(s)>2$, 从而所考虑的每个级数均绝对收敛. 像上面那样 $f_i(\frac{-1}{\tau},s)=\sum_{(m,n)\in Y_i}(\frac{\tau}{-n+m\tau})^s$. 然而如果 $(m,n)\in Y_0$, 则 $(\frac{\tau}{-n+m\tau})^s=\frac{\tau^s}{(-n+m\tau)^s}$, 并由于 $(m,n)\mapsto(-n,m)$ 诱导了从 Y_0 到 Y_1 的双射,, 从而推出 $f_0(\frac{-1}{\tau},s)=\tau^s f_1(\tau,s)$. 同样地, 如果 $(m,n)\in Y_1$, 则有 $(\frac{\tau}{-n+m\tau})^s=e^{-i\pi s}\frac{\tau^s}{(n-m\tau)^s}$, 并由于 $(m,n)\mapsto(n,-m)$ 诱导了从 Y_1 到 Y_0 的双射, 由此得到 $f_1(\frac{-1}{\tau},s)=e^{-i\pi s}\tau^s f_0(\tau,s)$. 如果 $\mathrm{Re}(s)>2$, 则所要的结果借助于公式 $E(\frac{-1}{\tau},s)=f_0(\frac{-1}{\tau},s)+f_1(\frac{-1}{\tau},s)$ 得到.

一般情形由解析延拓的唯一性得到 (这两项是 $\mathbf{C}$ 上的亚纯函数, 但它们在半平面 Ω_2 上重合; 它们的差因而恒等于 0).

(iv) 利用公式 $\lim_{s\to 2}(s-2)f_0(\tau,s)=\frac{1}{\tau}$ 得到 $\lim_{s\to 2}(e^{-i\pi s}-1)f_0(\tau,s)=-i\pi\frac{1}{\tau}$, 那么由此, 并从 (iii) 出发取极限便得到我们想要的公式.

问题 8. (i) 如果 $\mathrm{Im}(\tau)>a$, 则有 $|-e^{2i\pi n\tau}|\leqslant e^{-2\pi na}$. 由此得知由 $-e^{2i\pi n\tau}$ 构成的级数在半平面 $\mathrm{Im}(\tau)>a(a>0)$ 上按范数收敛, 从而乘积 $\prod_{n=1}^{+\infty}(1-e^{2i\pi n\tau})$ 收敛, 因而根据定理 V.5.4, 在此半平面上定义了一个全纯函数. 又由于其中没有一项取零, 故如此定义的函数也不取零. 将 $\mathscr{H}$ 写成这些半平面 $\mathrm{Im}(\tau)>a(a>0)$ 的并便得到结论.

(ii) 由于 η 是在可缩开集 $\mathscr{H}$ 上不取零的一个全纯函数, 故存在在 $\mathscr{H}$ 上的全纯函数 g 使得 $e^g=\eta$. 另外, 级数 $\frac{i\pi\tau}{12}+\sum_{n=1}^{+\infty}\log(1-e^{2i\pi n\tau})$ 在整个半平面 $\mathrm{Im}(\tau)>a$ 上收敛, 因而定义了 $\mathscr{H}$ 上的一个全纯函数 h. 然而以这个级数的部分和作指数就是 η 的部分乘积; 取极限便证明了 $e^h=\eta$. 由此推出 $g-h$ 是 $\mathscr{H}$ 上的取值于 $2i\pi\mathbf{Z}$ 中的全纯函数; 因而它是常数 (由其像的连通性, 或者由开映像定理), 便得结论.

(iii) 由于 $\lim_{s\to 0}\frac{1}{s}\frac{1}{\Gamma(s)}=1$, 故有 $F(\tau)=C+\sum_{k=1}^{+\infty}\sigma_{-1}(k)e^{2i\pi k\tau}$, 其中 $C=\zeta'(0)$. 通过变量变换 $d=\ell,k=\ell n$ 将和 $\sum_{n=1}^{+\infty}\sum_{\ell=1}^{+\infty}$ 转化为 $\sum_{k=1}^{+\infty}\sum_{d|k}$, 便得到了结果.

(iv) 对恒等式 $E(\frac{-1}{\tau},s)=\tau^s(E(\tau,s)+(e^{-i\pi s}-1)f_0(\tau,s))$ 关于 s 取导数并在 0 取值, 于是得到 $F(\frac{-1}{\tau})=(\log\tau)E(\tau,0)+F(\tau)-i\pi f_0(\tau,0)$, 利用问题 4.(v) 和问题 6.(iv) 的公式 $E(\tau,0)=\frac{-1}{2}$ 和 $f_0(\tau)=\frac{1}{12\tau}+\frac{\tau}{12}-\frac{1}{4}$ 可将上式改写为 $F(\frac{-1}{\tau})+\frac{i\pi}{12\tau}=-\frac{1}{2}\log+\tau F(\tau)-\frac{i\pi\tau}{12}+\frac{i\pi}{4}$. 于是第一个公式由 (iii) 得到; 而在两端取指数便得到了第二个公式.

(v) 对 (iii) 中的恒等式求导得到 $\frac{\eta'(\tau)}{\eta(\tau)}=-F'(\tau)+\frac{i\pi}{12}$. 另外, 由于一个全纯函数的收敛级数可以逐项求导, 故有 $F'(\tau)=2i\pi\sum_{k=1}^{+\infty}k\sigma_{-1}(k)e^{2i\pi k\tau}$. 但因为 $d\mapsto\frac{k}{d}$ 诱导了 k 的因子间的双射, 故 $k\sigma_{-1}(k)=\sum_{d|k}\frac{k}{d}=\sigma_1(k)$. 由此得到 $F'(\tau)=\frac{-1}{2i\pi}(E(\tau,2)-\zeta(2))$, 因而 $\frac{\eta'(\tau)}{\eta(\tau)}+\frac{1}{2i\pi}E(\tau,2)=\frac{i\pi}{12}+\frac{1}{2i\pi}\zeta(2)$.

现在, 如果对 (iv) 的恒等式求导, 则得到关系式 $\frac{1}{\tau^2}\frac{\eta'(\frac{-1}{\tau})}{\eta(\frac{-1}{\tau})}=\frac{1}{2\tau}+\frac{\eta'(\tau)}{\eta(\tau)}$. 利用问题 7 的 (iv) 便得知函数 $h(\tau)=\frac{\eta'(\tau)}{\eta(\tau)}+\frac{1}{2i\pi}E(\tau,2)$ 满足函数方程 $h(\frac{-1}{\tau})=\tau^2h(\tau)$. 按前面所说, h 是常值, 这意味着 $h=0$, 从而 $\frac{i\pi}{12}+\frac{1}{2i\pi}\zeta(2)=0$. 故有结果. [618]

问题 9. (i) 变量变换 $t=\sqrt{\frac{12}{y}}u$(或者是伸缩平移公式) 给出了

$$\int_{\mathbf{R}} e^{-2i\pi tx}e^{-2i\pi\frac{at}{12}}e^{-\pi\frac{yt^2}{12}}dt=\sqrt{\frac{12}{y}}\int_{\mathbf{R}} e^{-2i\pi\sqrt{\frac{12}{y}}(x+\frac{a}{12})u}e^{-\pi u^2}du$$
$$=\sqrt{\frac{12}{y}}e^{-\pi\frac{12}{y}(x+\frac{a}{12})^2}=\sqrt{\frac{12}{y}}e^{-\frac{\pi}{12y}(12x+a)^2}.$$

于是公式 $\sum_{n\in\mathbf{Z}}e^{-2i\pi\frac{an}{12}}e^{-\pi\frac{yn^2}{12}}=\sqrt{\frac{12}{y}}\sum_{n\in\mathbf{Z}}e^{-\frac{\pi}{12y}(12n+a)^2}$ 恰好是对于属于 $\mathscr{S}(\mathbf{R})$ 的函数 $t\mapsto e^{-2i\pi\frac{at}{12}}e^{-\pi\frac{yt^2}{12}}$ 的泊松公式.

(ii) 我们有 $\sum_{a=-5}^{6}\chi(a)e^{-2i\pi\frac{an}{12}}=2(\cos\frac{n\pi}{6}-\cos\frac{5n\pi}{6})$, 而所要结果来自

$$\cos\frac{n\pi}{6}=\cos\frac{5n\pi}{6}=\begin{cases}1, & n\equiv 0 \mod 12,\\ -1, & n\equiv 6 \mod 12,\\ 0, & n\equiv \pm 3 \mod 12,\\ \frac{1}{2}, & n\equiv \pm 2 \mod 12,\\ \frac{-1}{2}, & n\equiv \pm 4 \mod 12\end{cases}$$

和

$$\cos\frac{n\pi}{6}=-\cos\frac{5n\pi}{6}=\begin{cases}\frac{\sqrt{3}}{2}, & n\equiv \pm 1 \mod 12,\\ \frac{-\sqrt{3}}{2}, & n\equiv \pm 5 \mod 12.\end{cases}$$

(iii) 我们有 $H(iy)=\frac{1}{2}\sum_{n\in\mathbf{Z}}\chi(n)e^{-\pi\frac{n^2y}{12}}=\frac{1}{2\sqrt{12}}\sum_{n\in\mathbf{Z}}(\sum_{a=-5}^{6}\chi(a)e^{-2i\pi\frac{an}{12}})e^{-\pi\frac{n^2y}{12}}$, 利用 (i) 和此级数的绝对收敛性可将它重写为 $\frac{1}{2\sqrt{y}}\sum_{a=-5}^{6}\chi(a)\sum_{n\in\mathbf{Z}}e^{-\pi\frac{(12n+a)^2}{12y}}$.

另外, $\chi(12\pi+a)=\chi(a)$ 且映射 $(a,n)\mapsto 12n+a$ 是从 $\{-5,\ldots,6\}\times\mathbf{Z}$ 到 $\mathbf{Z}$ 的一个双射, 这样可将最后的这个和重写为 $\frac{1}{2\sqrt{y}}\sum_{m\in\mathbf{Z}}\chi(m)e^{-\pi\frac{m^2}{12y}}=\frac{1}{\sqrt{y}}H(\frac{i}{y})$. 因此对于 $y\in\mathbf{R}_+^*$, 我们有 $H(\frac{i}{y})=\sqrt{y}H(iy)$.

现在, 函数 $\tau\mapsto H(\frac{-1}{\tau})-\sqrt{\frac{\tau}{i}}H(\tau)$ 在 $\mathscr{H}$ 上全纯, 并根据前面所证在 $i\mathbf{R}_+^*$ 上为零. 因此根据孤立零点定理它恒等于 0. 得证.

(iv) $J(\frac{-1}{\tau})=J(\tau)$ 来自 (iii) 和问题 8 的 (iv). 另外, $e^{-i\pi\tau/12}\eta(\tau)$ 是周期为 1 的周期函数: 因为乘积的每一项是这样的. 同样由于 $\frac{(6n+1)^2-1}{12}=3n^2+n$ 是偶数, 故 $e^{-i\pi T/12}H(\tau)=\frac{1}{2}\sum_{n\in\mathbf{Z}}(-1)^ne^{-i\pi\frac{(6n+1)^2-1}{12}}$ 也是一个周期为 1 的周期函数. $e^{-i\pi\tau/12}H(\tau)$ 对于 $e^{-i\pi\tau/12}\eta(\tau)$ 的商就是 $J(\tau)$, 因此也是周期为 1 的周期函数, 故得结论.

(v) 我们有 $J(\tau)=\tilde{J}(e^{2i\pi\tau})$, 其中 $\tilde{J}(q)$ 是 $\sum_{n\in\mathbf{Z}}(-1)^nq^{(3n^2+n)/2}$ 对于 $\prod_{n\geqslant 1}(1-q^n)$ 的商, 其中前者是在 $D(0,1^-)$ 上的全纯函数 (利用定理 V.5.1), 而后者是一个不在 $D(0,1^-)$ 上取零的全纯函数 (参看定理 V.5.4). 因此它是一个 $D(0,1^-)$ 上的全纯函数. 在这些级数和乘积中令 $q=0$ 便看出 $\tilde{J}(0)=1$.

(vi) 由于 $\tilde{J}(0)=1$, 故函数 $q\to q^{-1}(\tilde{J}(q)-1)$ 在 $q=0$ 有一个极限 ℓ. 这等于说当 $\mathrm{Im}(\tau)\to+\infty$ 时 $\tau\mapsto e^{-2i\pi\tau}(J(\tau)-1)$ 趋向 ℓ. 因此存在 $M>0$ 使得如果 $\mathrm{Im}(\tau)>M$, 则有 $|J(\tau)-1)|\leqslant(|\ell|+1)e^{-2\pi\mathrm{Im}(\tau)}$. 由于连续函数 $\tau\mapsto e^{2\pi\mathrm{Im}(\tau)}|J(\tau)-1|$ 在 $\bar{X}\cap\{\tau,\mathrm{Im}(\tau)\leqslant M\}$ 上有界, 这表明 $e^{2\pi\mathrm{Im}(\tau)}|J(\tau)-1|$ 在 $\bar{X}$ 上有界, 因而存在 $c>0$ 使得 $|J(\tau)-1|\leqslant ce^{-2\pi\mathrm{Im}(\tau)}$, 其中 $\tau\in\bar{X}$.

假设 $J-1$ 在 $\bar{X}$ 上不恒为零, 且 τ_0 满足 $|J(\tau_0)-1|>0$. 于是选取 M 使得 $ce^{-2\pi M}<|J(\tau_0)-1|$ 以致当 $\mathrm{Im}(\tau)\geqslant M$ 时有 $|J(\tau)-1|<|J(\tau_0)-1|$. 于是 $|J-1|$ 在 $\bar{X}$ 上的最大值与在紧集 $\bar{X}\cap\{\tau,\mathrm{Im}(\tau)\leqslant M\}$ 上的最大值相同, 而最大值原理表明它在此紧集的边界上达到. 由于在线段 $[\frac{-2}{3}+iM,\frac{2}{3}+iM]$ 上有 $|J(\tau)-1|<|J(\tau_0)-1|$, 故不在此线段上达到最大值, 这便证明了在 ∂X 上的一点达到.

(vii) 如果 τ 在半直线 $]\frac{-2+i}{3},\frac{-2}{3}+i\infty[$ 上, 则 $\tau+1\in X$. 同样地, 如果 τ 在半直线 $]\frac{2+i}{3},\frac{2}{3}+i\infty[$ 上, 则 $\tau-1\in X$. 如果 $\tau=x+iy\in[\frac{-2+i}{3},\frac{2+i}{3}]$, 则 $\frac{-1}{\tau}=\frac{-x+\frac{1}{3}}{x^2+\frac{1}{9}}=x'+iy'$ 满足 $y'>\frac{1}{3}$: 因为 $x^2+\frac{1}{9}\leqslant\frac{5}{9}<1$ 且 $|x'|<\frac{|x|}{x^2}\leqslant\frac{3}{2}$; 由此可知, 三个数 $\frac{-1}{\tau},\frac{-1}{\tau}+1,\frac{-1}{\tau}-1$ 中至少有一个属于 X. [619]

设 $\tau_0\in\partial X$ 使得 $|J(\tau_0)-1|$ 达到 $|J-1|$ 的最大值. 由于 J 在数 $\tau_0+1,\tau_0-1,\frac{-1}{\tau_0},\frac{-1}{\tau_0}+1$ 和 $\frac{-1}{\tau_0}-1$ 的值与在 τ_0 的值相同, 并且其中有一个数属于 X, 故得知 $|J-1|$ 在开集 X 上达到最大. 根据最大值原理, 这表明 $J-1$ 为常值, 并由于 $\lim_{\tau\to i\infty}J(\tau)-1=0$, 根据孤立零点定理便证明了 $J-1$ 在 X 上, 从而在 $\mathscr{H}$ 上恒等于 0. 由此推出了我们想要证明的恒等式 $J=1$ 和 $\eta=H$.

问题 10. (i) 如果固定 $q\in D(0,1^-)$, 则级数 $\sum_{n\geqslant1}|q^{2n}|+|q^{2n-1}w|+|q^{2n-1}w^{-1}|$ 在 $\mathbf{C}^*$ 的每个紧集上按范数收敛, 因而根据定理 V.5.4, 这个乘积定义了 $\mathbf{C}^*$ 上的 w 的全纯函数.

(ii) $a_m(q)$ 的存在与唯一性是推论 VI.3.2 的特殊情形: 应用 $z_0=0,R_1=0$ 而 $R_2=+\infty$.

(iii) 当用 q^2w 去换 w 时, 我们失去了 $\prod_{n\geqslant1}(1+q^{2n-1}w)$ 中的项 $1+qw$, 但在 $\prod_{n\geqslant1}(1+q^{2n-1}w^{-1})$ 中添加了项 $1+q^{-1}w^{-1}$. 因此有 $A(q,q^2w)=\frac{1+q^{-1}w^{-1}}{1+qw}A(q,w)=q^{-1}w^{-1}A(q,w)$.

(iv) 我们有 $\sum_{m\in\mathbf{Z}}a_m(q)w^m=qwA(q,q^2w)=\sum_{m\in\mathbf{Z}}a_m(q)q^{2m+1}w^{m+1}$. 由此得到关系 $a_m(q)=q^{2m-1}a_{m-1}(q),m\in\mathbf{Z}$. 将 $a_m(q)$ 写成 $q^{m^2}b_m(q)$ 的形式, 于是这个关系成为了 $b_m(q)=b_{m-1}(q),m\in\mathbf{Z}$; 由此推出 $b_m(q)=b_0(q)=a_0(q)$, 其中 $m\in\mathbf{Z}$, 故得结论.

(v) 我们有 $A(e^{3i\pi\tau},-e^{i\pi\tau})=\prod_{n\geqslant1}(1-e^{i\pi3n\tau})(1-e^{i\pi(3n-1)\tau})(1-e^{i\pi(3n-2)\tau})=\prod_{k\geqslant1}(1-e^{i\pi k\tau})$, 因而, 如果 $\tau\in\mathscr{H}$, 则 $A(e^{3i\pi\tau},-e^{i\pi\tau})=e^{-i\pi\tau/12}\eta(\tau)$. 另外, 由 (ii) 和 (iv) 我们也得到 $A(e^{3i\pi\tau},-e^{i\pi\tau})=a_0(e^{3i\pi\tau})\sum_{m\in\mathbf{Z}}(-1)^m e^{i\pi(3m^2+m)/2}$, 从而如果 $\tau\in\mathscr{H}$, 则有 $A(e^{3i\pi\tau},-e^{i\pi\tau})=a_0(e^{3i\pi\tau})e^{-i\pi\tau/12}H(\tau)$. 由于根据问题 9 的 (vii), 在 $\mathscr{H}$ 上有 $H=\eta$, 这证明了 $a_0=1$; 由此得到三重乘积公式.

(vi) 利用其中 $q=e^{i\pi\tau}$ 和 $w=1$ 时的三重乘积公式, 并将 $1+q^{2n-1}$ 写为形如 $\frac{((1-q^{4n-2})(1-q^{4n}))(1-q^{2n})}{((1-q^{2n-1})(1-q^{2n}))(1-q^{4n})}$, 便给出了

$$\begin{aligned}&\prod_{n\geqslant 1}(1+q^{2n-1})\\=&(\prod_{n\geqslant 1}(1-q^{4n-2})(1-q^{4n}))(\prod_{n\geqslant 1}(1-q^{2n}))(\prod_{n\geqslant 1}(1-q^{2n-1})(1-q^{2n}))^{-1}(\prod_{n\geqslant 1}(1-q^{4n}))^{-1}\\=&(e^{-i\pi\tau/12}\eta(\tau))^2(e^{-i\pi\tau/24}\eta(\tau/2))^{-1}(e^{-i\pi\tau/6}\eta(2\tau))^{-1},\end{aligned}$$

由此推出

$$\begin{aligned}\theta(\tau)&=(\prod_{n\geqslant 1}(1-q^{2n}))(\prod_{n\geqslant 1}(1+q^{2n-1}))^2\\&=\frac{(e^{-i\pi\tau/12}\eta(\tau))^5}{(e^{-i\pi\tau/24}\eta(\tau/2))^2(e^{-i\pi\tau/6}\eta(2\tau))^2}\\&=\frac{\eta(\tau)^5}{\eta(2\tau)^2\eta(\tau/2)^2}.\end{aligned}$$

[620] H.12. $\zeta(3)$ 是无理数

本节的目的是要证明 (Apéry, 1979) $\zeta(3)=\sum_{k=1}^{+\infty}\frac{1}{k^3}$ 是个无理数[23]. 这里给出的证明取自 Nesterenko 重新编写过的 Apéry 的证明. 它借助于全纯函数的理论, 特别关键的是 Γ 函数的性质. 我们将特别重用斯特林公式 (命题 VII.2.9). 设 Ω 是半平面 $\{s\in\mathbf{C},\mathrm{Re}(s)>\frac{1}{4}\}$, 而 $g:\Omega\to\mathbf{C}$ 是函数 $z\mapsto z\log z-z$, 其中 log 是对数的主分支, 又令 $\varepsilon(z)=\log\Gamma(z)-g(z)+\frac{1}{2}\log z-\frac{1}{2}\log 2\pi$. 于是斯特林公式意味着存在 $C_1>0$ 使得对于所有 $z\in\Omega$ 有 $|\varepsilon(z)|\leqslant\frac{C_1}{|z|}$.

问题 1. 设 $Q_n(X)=\frac{(X-1)\cdots(X-n)}{X(X+1)\cdots(X+n)}$ 而 $R_n=Q_n^2$. 又设 $d_n=\mathrm{lcm}(1,2,\ldots,n)$.

(i) 证明由 $Q_n(X)=\sum_{i=0}^{n}\frac{a_i}{X+i}$ 定义的 a_i 属于 $\mathbf{Z}$.

(ii) 设 $\sum_{i=0}^{n}\frac{\alpha_1}{(X+i)^2}+\frac{\beta_i}{X+i}$ 是 R_n 的简单分式分解. 证明 $\alpha_i\in\mathbf{Z}$, $d_n\beta_i\in\mathbf{Z}$ 以及 $\sum_{i=0}^{n}\beta_i=0$.

(iii) 设 $S_n=\sum_{k=1}^{+\infty}(-R_n'(k))$. 证明 $S_n=u_n\zeta(3)-\frac{v_n}{d_n^3}$, 其中 $u_n,v_n\in\mathbf{Z}$.

问题 2. 设 $F_n(s)=(\frac{\pi}{\sin\pi s})^2R_n(s)$.

(i) 证明 F_n 在 Ω 上亚纯, 并除在 $\geqslant n+1$ 的整数上为二阶极点外全纯, 并在每条包含在 Ω 中的竖直直线上的无限远速降.

(ii) 证明在 $s=k$ 的邻域中 $(\frac{\pi}{\sin\pi s})^2=\frac{1}{(s-k)^2}+O(1)$; 由此得到 F_n 在 $s=k$ 的留数的用 R_n 的一个表达式.

(iii) 证明, 如果 $\mathrm{Re}(s)=\frac{1}{2}+a, a\in\mathbf{Z}$ 或者 $s\in\Omega$ 且 $\mathrm{Im}(s)\geqslant 1$, 则 $|\frac{\pi}{\sin\pi x}|\leqslant\pi$.

[23] Apéry 的证明引用了大量的工作, 而这些工作的目的在于证明 $\zeta(5)$ 是无理数, 但却失败了.

(iv) 由此推出, 如果 $\frac{1}{2} \leqslant \mathrm{Re}(s) \leqslant n+\frac{1}{2}$, 或者 $s \in \Omega$ 而 $\mathrm{Re}(s)=\frac{1}{2}+a, a \in \mathbf{Z}$, 或者 $|\mathrm{Im}(s)| \geqslant 1$, 则 $|F_n(s)| \leqslant \frac{\pi^2}{|s|^2}$.

(v) 设 $C \in [\frac{1}{2}, n+\frac{1}{2}]$. 如果 N 是一个 $\geqslant n$ 的整数, 则以 $I_1(N), I_2(N), I_3(N)$ 和 $I_4(N)$ 记 $\frac{1}{2i\pi}F_n(s)ds$ 分别沿线段 $[C+iN, C-iN], [C-iN, N+\frac{1}{2}-iN], [N+\frac{1}{2}-iN, N+\frac{1}{2}+iN]$ 和 $[N+\frac{1}{2}+iN, C+iN]$ 上的积分, 计算 $\sum_{j=1}^{4} I_j(N)$; 并由此推出 $S_n=\frac{1}{2i\pi}\int_{C-i\infty}^{C+i\infty} F_n(s)ds$.

问题 3. 设 $c=\frac{1}{\sqrt{2}}$. 如果 $u \geqslant 1$ 而 $t \in \mathbf{R}$, 则令 $G(t,u)=\frac{\Gamma(1+(1-c)u^2-iut)}{\Gamma(1+(1+c)u^2+iut)}\Gamma(cu^2+iut)^2$. 又令 $\alpha_1=1-c, \beta_1=-it, m_1=1, \alpha_2=1+c, \beta_2=it, m_2=-1, \alpha_3=c, \beta_3=it, m_3=2$, 故而 $G(t,u)=\frac{\alpha_1u^2+\beta_1u}{\alpha_2u^2+\beta_2u}\prod_{i=1}^{3}\Gamma(\alpha_iu^2+\beta_iu)^{m_i}$. 定义 $\log G(t,u)$ 为 $\log G(t,u)=\log\frac{\alpha_1u^2+\beta_1u}{\alpha_2u^2+\beta_2u}+\sum_{i=1}^{3} m_i\log(\Gamma(\alpha_iu^2+\beta_iu))$, 而斯特林公式给出了

$$\log G(t,u)=g(t,u)-2\log u+\log 2\pi+r(t,u)+\varepsilon(t,u),$$

其中 g, ε 和 r 分别由 $g(t,u)=\sum_{i=1}^{3} m_i g(\alpha_iu^2+\beta_iu), \varepsilon(t,u)=\sum_{i=1}^{3} m_i\varepsilon(\alpha_iu^2+\beta_iu)$ 和 $r(t,u)=\frac{1}{2}\sum_{i=1}^{3} m_i'\log(\alpha_i+\frac{\beta_i}{u})$ 定义, 而 $m_1'=1, m_2'=-1, m_3'=-2$.

(i) 计算 $\frac{\Gamma(n+1-s)}{\Gamma(1-s)}$ 和 $\frac{\Gamma(n+1+s)}{\Gamma(s)}$; 由此并利用互补公式推出 $F_n(cn+i\sqrt{n}t)=G(t,\sqrt{n})^2$, 其中 $n \geqslant 1$.

(ii) 推出 $S_n=\frac{\sqrt{n}}{2\pi}\int_{-\infty}^{+\infty} G(t,\sqrt{n})^2dt$.

(iii) 证明当 $\alpha>0$ 而 $\beta \in i\mathbf{R}$ 时, 在 $+\infty$ 的邻域中有 $g(\alpha u^2+\beta u)=2\alpha u^2\log u+(\alpha\log\alpha-\alpha)u^2+2\beta u\log u+(\beta\log\alpha)u+\frac{\beta^2}{2\alpha}+O(\frac{1}{u})$. [621]

(iv) 证明 $\sum_{i=1}^{3} m_i\alpha_i=\sum_{i=1}^{3} m_i\beta_i=\sum_{i=1}^{3} m_i\beta_i\log\alpha_i=0$; 由此推出存在 $A \in \mathbf{R}$ 使得 $\lim_{u\to+\infty}\log G(t,u)-\delta u^2+2\log u=A-\gamma t^2$, 其中令 $\delta=\sum_{i=1}^{3} m_i\alpha_i\log\alpha_i$, $\gamma=\frac{1}{2}\sum_{i=1}^{3}\frac{m_i}{\alpha_i}$.

(v) 证明 $\delta=2\log(\sqrt{2}-1), \gamma=2\sqrt{2}$. 由此并由于对于所有 $u \geqslant 1, t \in \mathbf{R}$ 存在囿于上的不等式 $u^2e^{-\delta u^2}|G(t,u)| \leqslant C(1+|t|)|G(t,1)|$ (参看问题 5), 推出 $(\sqrt{2}-1)^{-4n}n^{3/2}S_n$ 当 $n \to +\infty$ 时趋向一个非零极限 B.

问题 4. (i) 设 $a>e$. 利用素数定理证明, 当 n 充分大时有 $d_n \leqslant a^n$. (如果 p 是个素数, 计算 $v_p(d_n)$.)

(ii) 证明 $(\sqrt{2}-1)^4e^3<1$. 由此推出 $\zeta(3)$ 为无理数. (考虑 $d_n^3S_n$.)

问题 5. 设 α_i, β_i 和 m_i 是在问题 3 中引进的那些量. 如果 $\alpha>0$ 和 $\beta \in i\mathbf{R}$, 定义 $H_{\alpha,\beta}: \mathbf{R} \to \mathbf{R}$ 为 $H_{\alpha,\beta}(v)=\mathrm{Re}((2\alpha+\beta v)\log(\alpha+\beta v))$. 以 h_t 记函数 $u \mapsto \mathrm{Re}(g(t,u))$.

(i) 证明 $H_{\alpha,\beta}'(0)=0$ 以及 $H_{\alpha,\beta}''(v)=\frac{-2\alpha\beta^4v^2}{(\alpha^2-\beta^2v^2)^2}$.

(ii) 证明对于所有 $w \geqslant 0$ 有 $I(w)=\sum_{i=1}^{3} m_i\frac{\alpha_i}{(2\alpha_i^2+w)^2} \geqslant 0$.

(iii) 如果 $v \in]0,1]$, 令 $H(v)=vh_t'(\frac{1}{v})$. 证明 $H(v)=\sum_{i=1}^{3} m_iH_{\alpha_i,\beta_i}(v)$; 因此推出 $H''(v) \leqslant 0$.

(iv) 证明, 对于所有 $u \geqslant 1$ 有 $h_t(u)-\delta u^2 \leqslant h_t(1)-\delta$.

(v) 证明存在 C_2, C_3 使得对所有 $u \geqslant 1$ 和 $t \in \mathbf{R}$ 有 $\mathrm{Re}(r(t,u)) \leqslant C_2$ 以及对于所有 $t \in \mathbf{R}$ 有 $\mathrm{Re}(r(t,1)) \geqslant -\log(1+|t|) - C_3$.

(vi) 由此推出存在 C, 使得对于所有 $u \geqslant 1$ 和 $t \in \mathbf{R}$ 有 $|u^2 e^{-\delta u^2} G(t,u)| \leqslant C(1+|t|)|G(t,1)|$.

问题校正

问题 1. (i) 我们有 $a_i = \lim_{X\to -i} \frac{(X-1)\cdots(X-n)}{X\cdots(X+i-1)(X+i+1)\cdots(X+n)} = \frac{(-1)^n(n+i)!}{i!(-1)^i i!(n-i)!} = (-1)^{n-i}\frac{(n+i)!}{n!i!}\frac{n!}{(n-i)!i!} = (-1)^{n-i}\binom{n+i}{i}\binom{n}{i}$, 这证明了 $a_i \in \mathbf{Z}$.

(ii) $\sum_{i=0}^n \frac{\alpha_i}{(X+i)^2} + \frac{\beta_i}{X+i} = (\sum_{i=0}^n \frac{a_i}{X+i})^2 = \sum_{i=0}^n \frac{a_i^2}{(X+i)^2} + \sum_{i\neq j}\frac{a_i a_j}{(X+i)(X+j)}$. 由于 $\frac{1}{(X+i)(X+j)} = \frac{1}{j-i}(\frac{1}{X+i} - \frac{1}{X+j})$, 由此得到 $\alpha_i = a_i^2 \in \mathbf{Z}$ 和 $\beta_i = 2\sum_{j\neq i}\frac{a_i a_j}{j-i}$. 又由于 $|j-i| \leqslant n$, 我们有 $\frac{d_n}{j-i} \in \mathbf{Z}$, 从而 $d_n\beta_i \in \mathbf{Z}$.

最后因为 R_n 为 -2 阶的, 故 $\sum_{i=0}^n \beta_i = 0$.

(iii) 我们有 $-R_n'(k) = \sum_{i=0}^n \frac{2\alpha_i}{(k+i)^3} + \frac{\beta_i}{(k+i)^2}$. 由此得到

$$
\begin{aligned}
S_n &= \sum_{i=0}^{n}(2\alpha_i(\sum_{k=1}^{+\infty}\frac{1}{(k+i)^3}) + \beta_i(\sum_{k=1}^{+\infty}\frac{1}{(k+i)^2}))\\
&= \sum_{i=0}^{+\infty}(2\alpha_i(\zeta(3) - \sum_{k=1}^{i}\frac{1}{k^3}) + \beta_i(\zeta(2) - \sum_{k=1}^{i}\frac{1}{k^2})).
\end{aligned}
$$

由于 $\sum_{i=0}^n \beta_i = 0$, 故 $\zeta(2)$ 不再出现, 从而得到 $S_n = u_n\zeta(3) - \frac{v_n}{d_n^3}$, 其中 $u_n = 2\sum_{i=0}^n \alpha_i \in \mathbf{Z}$, 而 $v_n = \sum_{i=0}^n(2\alpha_i(\sum_{k=1}^i \frac{d_n^3}{k^3}) + d_n\beta_i(\sum_{k=1}^i \frac{d_n^2}{k^2}))$, 其中所有的项因为 $k \leqslant i \leqslant n$ 表明 $k \mid d_n$ 均为整数.

问题 2. (i) 第一部分来自 $R_n(s)$ 在 $1,2,\ldots,n$ 的二重零点与 $(\frac{\pi}{\sin \pi x})^2$ 在这些点上的二重极点相互抵消. 在竖直直线上速降来自 R_n 在这样的直线上由于次数 $\leqslant 0$ 而有界, 又由于 $|\frac{1}{\sin(c+iT)}| \leqslant \frac{2}{e^{|T|}-e^{-|T|}}$, 以致 $\frac{\pi}{\sin\pi s}$ 在竖直直线上速降. [622]

(ii) 函数 $s \mapsto (\frac{\pi}{\sin\pi s})^2$ 为周期为 1 的周期函数; 因此只需证明在 0 的这个结果即可. 但有 $\frac{\pi}{\sin\pi s} = \frac{1}{s}\frac{1}{1-\frac{\pi^2 s^2}{6}+\cdots} = \frac{1}{s} + \frac{\pi^2 s}{6} + \cdots$, 从而 $(\frac{\pi}{\sin\pi s})^2 = \frac{1}{s^2} + \frac{\pi^2}{3} + \cdots$.

现在, $R_n(s) = R_n(k) + (s-k)R_n'(k) + \cdots$, 从而在 $s = k$ 的邻域中, $F_n(s) = \frac{R_n(k)}{(s-k)^2} + \frac{R_n'(k)}{s-k} + O(1)$; 由此得到 $\mathrm{Res}(F_n, k) = R_n'(k)$.

(iii) 如果 $\mathrm{Re}(s) = \frac{1}{2}+a, a \in \mathbf{Z}$, 则 $|\sin\pi s| = \frac{1}{2}|e^{\frac{i\pi}{2}+ia\pi-\pi\mathrm{Im}(a)} - e^{\frac{-i\pi}{2}-ia\pi+\pi\mathrm{Im}(s)}| = \frac{1}{2}|(-1)^a i(e^{-\pi\mathrm{Im}(s)} + e^{\pi\mathrm{Im}(s)})|$, 且由于几何平均数与算术平均数之间的关系知最后的一项 $\geqslant 1$.

如果 $|\mathrm{Im}(s)| \geqslant 1$, 则有 $|\sin\pi s| \geqslant \frac{1}{2}(e^{\pi|\mathrm{Im}(s)|} - e^{-\pi|\mathrm{Im}(s)|}) \geqslant \frac{1}{2}(e^{\pi} - e^{\pi}) \geqslant 1$.

(iv) 我们注意, 在所有的情形都有 $s \in \Omega$, 这表明, 如果 $i \in \{1,2,\ldots,n\}$, 则有 $|\frac{s-i}{s+i}| \leqslant 1$. 由于 $|s^2F_n(s)| = |\frac{\pi}{\sin\pi s}|^2|\frac{s-1}{s+1}\cdots\frac{s-n}{s+n}|^2$, 如果 $\mathrm{Re}(s) = \frac{1}{2}+a, a \in \mathbf{Z}$ 或者 $|\mathrm{Im}(s)| \geqslant 1$, 则由 (iii) 推出了所要的囿于上的不等式. 而对在带 $\frac{1}{2} \leqslant \mathrm{Re}(s) \leqslant \frac{1}{2}+n$

上的囿于上的不等式可将最大值原理用于在顶点为 $\frac{1}{2}-iT, n+\frac{1}{2}+iT, n+\frac{1}{2}-iT$ 和 $\frac{1}{2}+iT$ 的矩形上的函数 $s^2F_n(s)$, 并令 T 趋向 $+\infty$ 得到.

(v) 留数公式证明了 $\sum_{j=1}^4 I_j(N)=\sum_{k=n+1}^N R'_n(k)$ (如果 $k\in\{1,2,\ldots,n\}$, 则由于 $R'_n(k)=0$, 故它 $=\sum_{k=1}^N R'_n(k)$). 因此当 $N\to+\infty$ 时, $\sum_{j=1}^4 I_j(N)\to -S_n$. 除此以外每当 $N\to+\infty$ 时,

- $I_1(N)$ 趋向 $-\frac{1}{2i\pi}\int_{C-i\infty}^{C+i\infty}F_n(s)ds$,
- $|I_2(N)|\leqslant \frac{1}{2\pi}|N+\frac{1}{2}-C|\sup_{s\in[C-iN,N+\frac{1}{2}-iN]}|F_n(s)|\leqslant\frac{1}{2\pi}|N+\frac{1}{2}-C|\frac{\pi^2}{N^2}$, 因此 $I_2(N)\to 0$,
- 同样的理由, $I_4(N)\to 0$,
- $|I_3(N)|\leqslant\frac{1}{2\pi}2N\sup_{s\in[N+\frac{1}{2}-iN,N+\frac{1}{2}+iN]}|F_n(s)|\leqslant\frac{N}{\pi}\frac{\pi^2}{(N+\frac{1}{2})^2}$, 从而 $I_3(N)\to 0$.

取极限便给出了 $-S_n=-\frac{1}{2i\pi}\int_{C-i\infty}^{C+i\infty}F_n(s)ds$. 得证.

问题 3. (i) 我们有 $\frac{\Gamma(n+1-s)}{\Gamma(1-s)}=(-1)^n(s-1)\cdots(s-n)$ 和 $\frac{\Gamma(n+1+s)}{\Gamma(s)}=s(s+1)\cdots(s+n)$, 且由于 $\frac{\pi}{\sin\pi s}=\Gamma(s)\Gamma(1-s)$, 故得到 $F_n(s)=\left(\frac{\Gamma(n+1-s)}{\Gamma(1-s)}\right)^2\left(\frac{\Gamma(s)}{\Gamma(n+1+s)}\right)^2(\Gamma(s)\Gamma(1-s))^2=\left(\frac{\Gamma(n+1-s)}{\Gamma(n+1+s)}\Gamma(s)^2\right)^2$. 结果由将 s 换作 $cn+i\sqrt{n}t$ 得到.

(ii) 我们可以对问题 2 的 (v) 用于 $C=cn\in[\frac{1}{2},n+\frac{1}{2}]$ 的情形, 并且以 $s=cn+i\sqrt{n}t$ 对直线 $]C-i\infty,C+i\infty[$ 进行参数化, 其中 $t\in\mathbf{R}$; 由此便得到结果 (利用 (i) 给出 $F_n(cn+i\sqrt{n}t)$ 的表达式).

(iii) 由于 $g(\alpha u^2+\beta u)=(\alpha u^2+\beta u)(-1+\log(\alpha u^2)+\log(1+\frac{\beta}{\alpha u}))$, 展开 $(\alpha u^2+\beta u)(-1+2\log u+\log\alpha+\frac{\beta}{\alpha u}-\frac{\beta^2}{2\alpha^2u^2}+O(\frac{1}{u^3}))$ 便可得到结果.

(iv) 恒等式 $\sum_{i=1}^3 m_i\alpha_i=\sum_{i=1}^3 m_i\beta_i=0$ 可直接得到. 现在, 我们有 $\sum_{i=1}^3 m_i\beta_i\log\alpha_i=it(-\log(1-\frac{1}{\sqrt{2}})-\log(1+\frac{1}{\sqrt{2}})+2\log\frac{1}{\sqrt{2}})$, 并由于 $(1-\frac{1}{\sqrt{2}})(1+\frac{1}{\sqrt{2}})=\frac{1}{2}=(\frac{1}{\sqrt{2}})^2$, 故括号中为 0, 从而 $\sum_{i=1}^3 m_i\beta_i\log\alpha_i=0$. 于是 $g(t,u)-\delta u^2\to\sum_{i=1}^3 m_i\frac{\beta_i^2}{2\alpha_i}=-\gamma t^2$. 由此推出结果, 其中因为当 $i\in\{1,2,3\}$ 时 $\varepsilon(\alpha_iu^2+\beta_iu)\to 0$, 故有结果, 其中 $A=\log 2\pi+\frac{1}{2}\sum_{i=1}^3 m'_i\log\alpha_i$.

(v) 按照在 (iv) 中所做的计算, 我们有 $\delta=(1-c)\log(1-c)-(1+c)\log(1+c)+2c\log c=\log(1-c)-\log(1+c)$, 并由于 $\frac{1-c}{1+c}=\frac{\sqrt{2}-1}{\sqrt{2}+1}=(\sqrt{2}-1)^2$, 得到了第一个公式, 至于第二个, 注意到 $\frac{1}{1-c}-\frac{1}{1+c}+\frac{2}{c}=\frac{2c}{1-c^2}+2\sqrt{2}=4\sqrt{2}$, 这便给出了 $\gamma=2\sqrt{2}$.

现在, 当 $t\to+\infty$ 时, $u^4e^{-2\delta u^2}G(t,u)^2\to e^{2A}e^{-2\gamma t^2}$. 由于

$$|u^4e^{-2\delta u^2}G(t,u)^2|\leqslant C^2(1+|t|)^2|G(t,1)|^2=C^2(1+|t|)^2|F_1(c+it)|,$$

并因为 F_1 在竖直直线 $c+i\mathbf{R}$ 上速降 (参看问题 2.(i)), 交换极限与积分 (根据控制收敛定理这是合理的) 便得到 $u^4(\sqrt{2}-1)^{-4u^2}\int_{-\infty}^{+\infty}G(t,u)^2dt\to e^{2A}\int_{-\infty}^{+\infty}e^{-4\sqrt{2}t^2}dt$(最后的这个积分值等于 $B'=e^{2A}\sqrt{\frac{\pi}{4\sqrt{2}}}$). 令 $u=\sqrt{n}$ 并利用 (ii) 便得到结果, 其中 $B=B'/2\pi e^{2A}$.

[623] **问题 4.** (i) 如果 $p^v \mid d_n$, 则存在 $i \in \{1,\ldots,n\}$ 使得 $p^v \mid i$; 特别地, $p^v \leqslant n$. 由此得到 $v_p(d_n) = [\frac{\log n}{\log p}]$. 因此有 $\log d_n = \sum_{p\leqslant n}[\frac{\log n}{\log p}]\log p \leqslant (\log n)|\{p, p\leqslant n\}|$, 由此并由素数定理得到, 当 n 充分大时有 $\log d_n \leqslant n\log a$.

(ii) 我们有 $(\sqrt{2}-1)^4 e^3 = \frac{e^3}{(\sqrt{2}+1)^4} = \frac{e^3}{(3+2\sqrt{2})^2} = \frac{e^3}{17+12\sqrt{2}} \leqslant \frac{3^3}{17+12} < 1$. 如果 $\zeta(3)$ 是个有理数, 可写其为 $\frac{a}{N}$ 形式, 那么当 $n \geqslant N$ 时, 由于 d_n^3 被 N 整除, 从而 $d_n^3 S_n = d_n^3 u_n\zeta(3) - v_n$ 为整数. 另外, 由于当 n 充分大时 $S_n \sim Bn^{-3/2}(\sqrt{2}-1)^{4n}, B\neq 0$, 故当 n 充分大时, $d_n^3 S_n$ 是一个非零整数. 我们可以选取 $a > e$ 使得 $b = a^3(\sqrt{2}-1)^4 < 1$, 从而根据 (i), 对于所有充分大的 n 有 $|d_n^3 S_n| \leqslant Bn^{-3/2}b^n$, 因此 $d_n^3 S_n \to 0$. 因为一个非零的整数序列不可能趋向 0, 故引出了矛盾从而得到结果.

问题 5. (i) $H'_{\alpha,\beta}(v) = \mathrm{Re}(\beta\log(\alpha+\beta v) + \frac{\alpha\beta}{\alpha+\beta v} + \beta)$, 从而因为 $\beta \in i\mathbf{R}$ 和 $\alpha > 0$, 故有 $H'_{\alpha,\beta}(0) = 0$. 最后,

$$H''_{\alpha,\beta}(v) = \mathrm{Re}\left(\frac{\beta^2}{\alpha+\beta v} - \frac{\alpha\beta^2}{(\alpha+\beta v)^2}\right) = \beta^2\left(\frac{\alpha}{\alpha^2-\beta^2 v^2} - \frac{\alpha(\alpha^2+\beta^2 v^2)}{(\alpha^2-\beta^2 v^2)^2}\right) = \frac{-2\alpha\beta^4 v^2}{(\alpha^2-\beta^2 v^2)^2}.$$

(ii) 我们有 $I(w) = \frac{1}{\sqrt{2}}(\frac{\sqrt{2}-1}{(3-2\sqrt{2}+w)^2} - \frac{\sqrt{2}+1}{(3+2\sqrt{2}+w)^2} + \frac{2}{(1+w)^2})$. 在通分后, 我们看出 $I(w)$ 与下面的表达式有相同的符号:

$$(1+w)^2((\sqrt{2}-1)(3+2\sqrt{2}+w)^2 + (-\sqrt{2}-1)(3-2\sqrt{2}+w)^2) + 2(3+2\sqrt{2}+w)^2(3-2\sqrt{2}+w)^2$$

$$= 2((1+w)^2(-w^2+2w+7) + (1+6w+w^2)^2) = 2(12w^3+32w^2+44w+8)$$

对于所有 $w \geqslant 0$, 故 $\geqslant 0$.

(iii) 有 $g(t,u) = \sum_{i=1}^3 m_i g(\alpha_i u^2 + \beta_i u)$; 由于 g 的导数是 log, 那么 $g(t,u)$ 对于 u 的导数是 $\sum_{i=1}^3 m_i(2\alpha_i u + \beta_i)\log(\alpha_i u^2 + \beta_i u)$, 因此

$$H(v) = \mathrm{Re}\left(\sum_{i=1}^3 m_i(2\alpha_i + \beta_i v)(\log(\alpha_i + \beta_i v) - 2\log v)\right).$$

因为 $\sum_{i=1}^3 m_i\alpha_i = \sum_{i=1}^3 m_i\beta_i = 0$, 故上面含 $\log v$ 的项消失, 剩余的是 $H(v) = \sum_{i=1}^3 m_i H_{\alpha_i,\beta_i}(v)$.

由于当 $i = 1,2,3$ 时 $\beta_i^2 = -t^2$, 故得到 $H''(v) = -8t^4v^2 I(2t^2v^2)$, 因此根据 (ii) 有 $H''(v) \leqslant 0$.

(iv) 根据 (i) 有 $H'(0) = 0$, 又根据 (iii), $H''(v) \leqslant 0$; 因此当 $v \in]0,1]$ 时有 $H'(v) \leqslant 0$. 由于 $H(0) = 2\sum_{i=1}^3 m_i\alpha_i\log\alpha_i = 2\delta$, 故当 $v \in]0,1]$ 时有 $H(v) \leqslant 2\delta$, 从而 $h_t'(u) - 2\delta u \leqslant 0$, 其中 $u \geqslant 1$. 函数 $u \mapsto h_t(u) - \delta u^2$ 因而递降. 得证.

(v) 我们有 $\mathrm{Re}(r(t,u)) = \frac{1}{2}\log|\frac{1-c-i\frac{t}{u}}{1+c+i\frac{t}{u}}| - \log|c + i\frac{t}{u}|$; 特别地, 因为已经知道 $|\alpha + i\frac{t}{u}|(\alpha \in \{1-c, 1+c, c\})$ 只依赖 $x = \frac{t^2}{u^2}$, 故它更是如此. 又由于当 $x \to +\infty$ 时它趋向 $-\infty$ 并在 $\mathbf{R}_+$ 上连续, 故得到了 C_2 的存在性.

由于 $t \mapsto \frac{1-c-it}{1+c+it}$ 有界并不趋向 0, 故 C_3 的存在性来自 $t \mapsto \log|\frac{1-c-it}{1+c+it}|$ 的有界性, 并且因为 $t \mapsto \frac{c+it}{1+|t|}$ 有界, 于是 $t \mapsto -\log|c+it| + \log(1+|t|)$ 也有界.

(vi) 我们有 $\log|\frac{u^2 e^{-\delta u^2} G(t,u)}{G(t,1)}| = -\delta u^2 + h_t(u) - h_t(1) + \mathrm{Re}(r(t,u) - r(t,1)) + \mathrm{Re}(\varepsilon(t,u) - \varepsilon(t,1))$. 然而

- 根据 (iv), $h_t(u) - \delta u^2 - h_t(1) \leqslant -\delta$,
- 根据 (v), $\mathrm{Re}(r(t,u) - r(t,1)) \leqslant C_2 + C_3 + \log(1+|t|)$,
- $\varepsilon(t,u) = \sum_{i=1}^{3} m_i \varepsilon(\alpha_i + \beta_i u)$, 并由于当 $u \geqslant 1, t \in \mathbf{R}$ 和 $i = 1,2,3$ 时有 $|\alpha_i + \beta_i u| \geqslant 1 - c$, 根据在前言中回顾的斯特林公式得到了 $\mathrm{Re}(\varepsilon(t,u) - \varepsilon(t,1)) \leqslant 2(\sum_{i=1}^{3} |m_i|) \frac{C_1}{1-c}$.

结果由令 $C = \exp(\delta + C_2 + C_3 + \frac{8C_1}{1-c})$ 得到.

H.13. 博雷尔判别准则 [624]

设 f 是 $D(0, r^-)(r > 1)$ 上的亚纯函数, 它在 0 全纯. 设 f 在 0 的泰勒展开式为 $\sum_{n=0}^{+\infty} a_n z^n$. 我们要证明, 如果这些 a_n 是整数, 则 f 是一个有理分式 (博雷尔, 1894). 证明由两部分组成: 第 I 部分给出了一个形式级数为有理分式的纯代数的判别法; 第 II 部分则利用全纯函数的性质证明, 我们所感兴趣的情形满足可以应用第 I 部分的判别法的条件.

第 I 部分

设 K 为域, $(a_n)_{n\in\mathbf{N}}$ 是 K 中的序列. 以 $F \in K[[T]]$ 记形式级数 $\sum_{n\in\mathbf{N}} a_n T^n$, 我们想要建立一个判别法以确定 F 是否是一个有理分式 (或者更准确地说是一个有理分式在原点的泰勒展开式).

如果 $N \geqslant 1, n \in \mathbf{N}$, 令 $A_N(n) = (a_n, a_{n+1}, \ldots, a_{n+N-1}) \in K^N$, 并令 $\Delta_N(n)$ 为汉克尔 (Hankel) 行列式 $\det(A_N(n), \ldots, A_N(n+N-1))$ (因此, $\Delta_N(n) = \det(a_{n+i+j})_{0\leqslant i,j\leqslant N-1}$).

(i) 设 $c_1, \ldots, c_N \in K$ 而 $P = 1 + c_1 T + \cdots + c_N T^N$. 证明下列等价:

- 存在 $Q \in K[T]$ 使得 $F = \frac{Q}{P}$;
- 存在 $n_0 \in \mathbf{N}$ 使得对于所有 $n \geqslant n_0$ 有 $a_{n+N} + c_1 a_{n+N-1} + \cdots + c_N a_n = 0$.

由此我们推出, 如果 F 是个有理分式, 则存在 $M \geqslant 1$ 和 $m_0 \in \mathbf{N}$ 使得对于所有 $n \geqslant m_0$ 有 $\Delta_M(n) = 0$.

(ii) 假设 $\Delta_{N+1}(n) = 0$ 而 $\Delta_N(n+1) \neq 0$. 证明 $\Delta_N(n) \neq 0$. (可以考虑矩阵 $B = (a_{n+i+j})_{0\leqslant i,j\leqslant N}$, 其中 $A_N(n+i)$ 是其子矩阵的行和列, 并证明 $A_N(n+N)$ 属于 K^N 中由 $A_N(n), \ldots, A_N(n+N-1)$ 生成的子空间.)

(iii) 假设存在 $M \geqslant 1$ 和 $m_0 \in \mathbf{N}$ 使得当对所有 $n \geqslant m_0$ 时有 $\Delta_M(n) = 0$. 证明存在 $N, n_0 \in \mathbf{N}$, 使得对所有 $n \geqslant n_0$ 有 $\Delta_{N+1}(n) = 0$ 和 $\Delta_N(n) \neq 0$.

(iv) 证明 $A_N(n_0+N) + c_1 A_N(n_0+N-1) + \cdots + c_N A_N(n_0) = 0$, 其中 $c_1, \ldots, c_N \in$

K 唯一确定, 并证明有 $A_N(n+N) + c_1 A_N(n+N-1) + \cdots + c_N A_N(n) = 0$ 对所有 $n \geqslant n_0$ 都成立. 如何将其翻译成有关序列 $(a_n)_{n\in\mathbf{N}}$ 的陈述?

(v) 证明如果存在 $M \geqslant 1$ 和 $m_0 \in \mathbf{N}$ 使得对于所有 $n \geqslant m_0$ 有 $\Delta_M(n) = 0$, 则 F 是个有理分式. □

第 II 部分

设 f 是 $D(0,r^-), r > 1$ 上的一个亚纯函数, 并在 0 全纯. 设 $\sum_{n=0}^{+\infty} a_n z^n$ 为 f 在 0 的泰勒展开式.

(i) 设 $R \in]1, r[$. 证明 f 在 $D(0,R)$ 中只有有限个极点 (计入重数).

(ii) 证明存在 $R_0 > 0$ 和 $C_0 > 0$, 使得对所有 $n \in \mathbf{N}$ 有 $|a_n| \leqslant C_0 R_0^{-n}$.

(iii) 设 $c_1, \ldots, c_d \in \mathbf{C}$ 由 $1 + c_1 X + \cdots + c_d X^d = \prod_{j=1}^{d}(1 - \alpha_j^{-1} X)$ 定义. 证明存在 $C > 0$ 和 $R > 1$ 使得对于所有 $n \in \mathbf{N}$ 有 $|a_{n+d} + c_1 a_{n+d-1} + \cdots + c_d a_n| \leqslant C R^{-n}$. (可以关注函数 $f(z)\prod_{j=1}^{d}(1 - \alpha_j^{-1} z)$.)

(iv) 推导: 存在 $N \geqslant 1$ 和 $n_0 \in \mathbf{N}$ 使得对于所有 $n \geqslant n_0$ 有 $|\Delta_N(\boldsymbol{a}, n)| < 1$. (可以找出 $B_N(n+i) = A_N(n+i+d) + c_1 A_N(N+i+d-1) + \cdots + c_d A_N(n+i)$ 的坐标的上界.)

(v) 证明当 a_n 是整数时 f 是一个有理函数. □

[625]

问题校正

第 I 部分

(i) 我们有 $(1 + c_1 T + \cdots + c_N T^N)F(T) = \sum_{n\in\mathbf{N}} b_n T^n$, 其中 $b_{n+N} = a_{n+N} + c_1 a_{n+N-1} + \cdots + c_N a_n$; 由此看出 $(1 + c_1 T + \cdots + c_N T^N)F(T)$ 是一个多项式当且仅当对于充分大的 n 有 $a_{n+N} + c_1 a_{n+N-1} + \cdots + c_N a_n = 0$. 因此问题中的两个条件等价.

现在, 如果 F 为有理函数, 则可将其写成 $F = \frac{Q}{P}$, 其中 P, Q 为互素的首 1 多项式. 由于 F 在 0 没有极点, 故 $P(0) \neq 0$, 并且必要时可用 $P(0)$ 除以 P 和 Q, 故不妨设 $P(0) = 1$, 因此 $P = 1 + c_1 T + \cdots + c_N T^N$. 按照前面的讨论, 因此存在 $n_0 \in \mathbf{N}$ 使得对所有 $n \geqslant n_0$ 有 $a_{n+N} + c_1 a_{n+N-1} + \cdots + c_N a_n = 0$. 因此对所有的 $n \geqslant n_0$ 有 $c_1 A_{N+1}(n+N-1) + \cdots + c_N A_{N+1}(n) = 0$. 因为 $A_{N+1}(n+N)$ 是 $A_{N+1}(n+N-1), \ldots, A_{N+1}(n)$ 的线性组合, 故对所有的 $n \geqslant n_0$ 有 $\Delta_{N+1}(n) = 0$. 那么让 $M = N+1, m_0 = n_0$ 便得到结论.

(ii) 假设条件 $\Delta_N(n+1) \neq 0$ 等价于 $A_N(n+1), \ldots, A_N(n+N)$ 是 K^N 的一组基; 这表明矩阵 B 的前 N 行 $A_{N+1}(n), \ldots, A_{N+1}(n+N-1)$ 是线性无关的. 因为 $\Delta_{N+1}(n) = 0$, 故 $A_{N+1}(n), \ldots, A_{N+1}(n+N-1)$ 是一个相关族, 因此可将 B 的最后一行 $A_{N+1}(n+N)$ 写成 $\lambda_N A_{N+1}(n) + \cdots + \lambda_1 A_{N+1}(n+N-1)$. 忽略掉最后一

列, 这便给出了关系式 $A_N(n+N)=\lambda_N A_N(n)+\cdots+\lambda_1 A_N(n+N-1)$, 这证明了 $A_N(n+N)$ 在 K^N 中由 $A_N(n),\ldots,A_N(n+N-1)$ 生成的子空间中; 由于这个空间包含了基 $A_N(n+1),\ldots,A_N(n+N)$, 故它等于 K^N. 换言之, $A_N(n),\ldots,A_N(n+N-1)$ 是 K^N 的一个生成元族, 而因为它有 N 个元, 故为一组基; 它的行列式 $\Delta_N(n)$ 因而非零, 这即为所要求证的.

(iii) 设 N 是使得存在一个 $n_0\in\mathbf{N}$, 对于所有 $n\geqslant n_0$ 有 $\Delta_{N+1}(n)=0$ 的最大整数. 于是存在无限多个 n 使得 $\Delta_N(n)\neq 0$, 而利用 (ii) 立即可归纳证明, 如果 $n_0\leqslant n'\leqslant n$ 和 $\Delta_N(n)\neq 0$, 则有 $\Delta_N(n')\neq 0$. 由于 n 可取得任意大, 故对所有的 $n\geqslant n_0$ 都有 $\Delta_N(n)\neq 0$. 结论得证.

(iv) 由于 $\Delta_N(n_0)\neq 0$, 故 $A_N(n_0),\ldots,A_N(n_0+N-1)$ 构成了 K^N 的一组基. 由此推出 $c_1,\ldots,c_N$ 的存在及唯一性. 现在, $A_{N+1}(n_0),\ldots,A_{N+1}(n_0+N)$ 成了一个无关族, 因而存在 $\lambda_1,\ldots,\lambda_N$ 使得 $A_{N+1}(n_0+N)+\lambda_1 A_{N+1}(n_0+N-1)+\cdots+\lambda_N A_{N+1}(n_0)=0$. 略去每个 $A_{N+1}(n_0+i)$ 的最后的一个坐标便得到 $A_N(n_0+N)+\lambda_1 A_N(n_0+N-1)+\cdots+\lambda_N A_N(n_0)=0$, 因此 $\lambda_1=c_1,\ldots,\lambda_N=c_N$. 现在略去第一个坐标, 我们得到了 $A_N(n_0+1+N)+c_1A_N(n_0+1+N-1)+\cdots+c_NA_N(n_0+1)=0$. 于是我们可以重新开始进行相同的推理, 但需将 n_0 换成 n_0+1, 便立即归纳地证明了对于 $n\geqslant n_0$ 有 $A_N(n+N)+c_1A_N(n+N-1)+\cdots+c_NA_N(n)=0$.

这个归纳关系等于说对于所有 $n\geqslant n_0$ 有 $a_{n+N}+c_1a_{n+N-1}+\cdots+c_Na_n=0$.

(v) 按照前面的这个问题, 存在 $N,n_0\in\mathbf{N}$ 使得对所有的 $n\geqslant n_0$ 有 $a_{n+N}+c_1a_{n+N-1}+\cdots+c_Na_n=0$. 令 $Q(T)=(1+c_1T+\cdots+c_NT^N)F(T)=\sum_{n\in\mathbf{N}}b_nT^n$. 于是当 $n\geqslant n_0+N$ 时, 因为 $b_{n+N}=a_{n+N}+c_1a_{n+N-1}+\cdots+c_Na_n$, 故 $b_n=0$; 这证明了 Q 是一个多项式 (次数 $<n_0+N$), 从而 $F=\frac{Q(T)}{1+c_1T+\cdots+c_NT^N}$ 是个有理分式. □

第 II 部分

(i) 如果 $\alpha\in D(0,R)$, 则存在 $r_\alpha>0$ 使得 f 在 $D(\alpha,r_\alpha^-)$ 中最多只有一个极点; 如果 α 是一个 k 阶极点, 则 $(z-\alpha)^kf$ 在 α 全纯并存在 $r_\alpha>0$ 使得 $(z-\alpha)^kf$ 在 $D(\alpha,r_\alpha^-)$ 上没有极点, 因而 f 在 $D(\alpha,r_\alpha^-)$ 上只在 α 有极点. $D(\alpha,r_\alpha^-)$ 构成了 $D(0,R)$ 的一个开覆盖, 并且 $D(0,R)$ 作为紧集, 可以从这个覆盖中抽出一个子覆盖 $D(\alpha,r_\alpha^-)$, [626] 其中 $\alpha\in A$ 为有限集. 因此 f 在 $D(0,R)$ 中只有 $\leqslant|A|$ 个极点, 而由于每个极点的阶数有限, 从而断言得证.

(ii) 由于 f 在 0 全纯, 于是它在一个圆盘 $D(0,R_1^-),R_1>0$ 中全纯. 如果 $0<R_0<R_1$, 我们从柯西不等式 (注记 V.4.9(iii)) 得到 $|a_n|\leqslant C_0R_0^{-n}$, 其中 $C_0=\sup_{|z|=R_0}|f(z)|$.

(iii) 设 $g(z)=f(z)\prod_{j=1}^d(1-\alpha_j^{-1}z)$, 而 $\sum_{n\in\mathbf{N}}b_nz^n$ 为其在 0 的泰勒级数; 因此有 $b_{n+d}=a_{n+d}+c_1a_{n+d-1}+\cdots+c_da_n$. 按构造, g 在 $D(0,r^-)$ 亚纯, 并因为它被

消去了可能出现在 $D(0,R)$ 中的极点, 故在 $D(0,R)$ 上全纯; 因此它在一个严格包含了 $D(0,R)$ 的开集 Ω 上全纯. 那么由柯西不等式我们得知, 存在 $C'>0$ 使得对每个 $n\in\mathbf{N}$ 成立 $|b_n|\leqslant C'R^{-n}$, 令 $C=C'R^{-d}$ 便得结论.

(iv) $\Delta_N(n)$ 是 $A_N(n),\ldots,A_N(n+N-1)$ 的行列式; 如果我们在 $A_N(n+i)$ 上添加 $A_N(n+j), j<i$ 的一个线性组合, 则不会改变此行列式. 因此 $\Delta_N(n)$ 也是 $A_N(n),\ldots,A_N(n+d-1),B_N(n),\ldots,B_N(n+N-1-d)$ 的行列式. 那么这个行列式是 $N!$ 个项的和, 其中每一项都是 d 个 $A_N(n+j)$ 的坐标分量和 $N-d$ 个 $B_N(n+i)$ 的坐标分量的乘积.

但是 $B_N(n+i)$ 的坐标是 $b_{n+i},\ldots,b_{n+i+N-1}$, 其中 $b_n=a_{n+d}+c_1a_{n+d-1}+\cdots+c_da_n$; 按照 (iii), 从绝对值上它们均小于 CR^{-n}. 另外, $A_N(n+j)$ 的坐标, 按照 (ii), 当 $0\leqslant j\leqslant d-1$ 时均小于 $C_0R_0^{-n-d-N+2}$. 于是得到囿于上的不等式 $|\Delta_N(n)|\leqslant N!(C_0R_0^{-n-d-N+2})^d(CR^{-n})^{N-d}$. 如果 $R^{N-d}R_0^d>1$, 那么, 当 $n\to+\infty$ 时, 这个囿于上的函数趋向 0. 因为这个条件当 N 充分大时满足, 断言得证.

(v) 如果这些 a_n 是整数, 那么 $\Delta_N(n)$ 也是整数, 而对于 $n\geqslant n_0$ 的不等式 $|\Delta_N(n)|<1$ 给出了当 $n\geqslant n_0$ 时 $\Delta_N(n)=0$. 故利用第 I 部分得到 f 为有理函数. □

[627] H.14. 莫德尔 – 韦伊定理

在这一节中[24], D 是一个无平方因子的奇整数. 如果 $S=\{p_1,\ldots,p_s\}$ 是整除 D 的素数的集合, 其中 s 是 S 的基数, 于是 $2\notin S$, 且 D 是这些 $p_i, 1\leqslant i\leqslant s$ 的乘积.

本节的目的是研究方程 $y^2=x^3-D^2x, x>0$ 的解 $(x,y)\in\mathbf{Q}^2$ 的集合 $C(\mathbf{Q})$. 更准确地说, 是要证明我们可以赋予 $\overline{C}(\mathbf{Q})=C(\mathbf{Q})\cup\{\infty\}$ 一个有限型的交换群结构 (莫德尔 – 韦伊定理的特殊情形). 以 C 记方程 $y^2=x^3-D^2x, x>0$ 在 $\mathbf{R}^2$ 中解的集合, 因此 $C(\mathbf{Q})=C\cap\mathbf{Q}^2$.

I

在这一部分中, Γ 是一个将运算记为 $+$ 的交换群. Γ 的中性元被记为 0 , 记 Γ 中元 x 的逆元为 $-x$. 如果 $n\in\mathbf{Z}, x\in\Gamma$, 则记 nx 为 Γ 中不说自明的元 ($0x=0$, 而 $(n+1)x=nx+x$, 其中 $n\in\mathbf{Z}$).

称 Γ 是有限型的是说存在 $r\in\mathbf{N}$ 和 $x_1,\ldots,x_r\in\Gamma$ 使得 Γ 中每一个元都可以写成 $\sum_{i=1}^r n_ix_i$ 的形式, 其中 $n_i\in\mathbf{Z}, 1\leqslant i\leqslant r$. 称 Γ 是 mod 2 有限型的, 则是说存在 Γ

[24]它是 2003 年巴黎高等师范学院的入学考试的 6 个小时的试题. 第 I 部分给出了证明一个交换群是有限型的判别法, 第 II 部分赋予 $\overline{C}=C\cup\{\infty\}$ 一个交换群的结构 (我们宁愿像在 H.8 中那样, 用全纯函数来达到目的), 第 III 部分给出了与此群运算相关的几个公式, 而第 IV 部分则致力于证明莫德尔 – 韦伊定理. 这四个部分建立在不同的技术之上, 可以独立地进行处理 (对于第 III 部分, 它只需要在第 II 部分的问题 6.b 给出的加法定义, 而第 IV 部分则以强化的方式利用了第 III 部分的公式而非它们的证明.

的一个有限子集 Z 使得 Γ 中每个元可以写成为 $z+2y$ 的形式, 其中 $z\in Z$ 而 $y\in\Gamma$.

Γ 上的一个高指的是这样一个映射 $h:\Gamma\to\mathbf{R}_+$: 存在 $M>0$ 使得对于任意的 $(x,y)\in\Gamma^2$ 有

$$|h(x+y)+h(x-y)-2h(x)-2h(y)|\leqslant M.$$

称 h 是容许的是说对于任意的 $B\geqslant 0$, Γ 中满足 $h(x)\leqslant B$ 的元 x 的集合为有限的.

1. 以 Γ_{tors} 记这样的 $x\in\Gamma$ 的集合, 它满足存在一个 $n\in\mathbf{Z}-\{0\}$ 使得 $nx=0$.

1.a. 证明 Γ_{tors} 是 Γ 的一个子群.

1.b. 群 Γ_{tors} 一定是有限的吗?

2. 设 h 是 Γ 上的一个高.

2.a. 证明, 如果 $x\in\Gamma$, 通项为 $4^{-n}h(2^nx)$ 的序列当 n 趋向 $+\infty$ 时趋向一个极限 $\hat{h}(x)$, 并且存在 $M'\geqslant 0$ 使得对于任意的 $x\in\Gamma$ 有 $|h(x)-\hat{h}(x)|\leqslant M'$.

2.b. 证明 $\hat{h}$ 对任意的 $x,y\in\Gamma$ 满足恒等式

$$\hat{h}(x+y)+\hat{h}(x-y)=2\hat{h}(x)+2\hat{h}(y).$$

2.c. 计算用 $\hat{h}(x)$ 表达的 $\hat{h}(nx)$, 其中 $n\in\mathbf{Z}$. [628]

3. 假设已赋予 Γ 一个容许高 h.

3.a. 证明 $\hat{h}$ 是 Γ 上的一个容许高.

3.b. 证明 $\hat{h}(x)=0$ 当且仅当 $x\in\Gamma_{\text{tors}}$.

3.c. 证明 Γ_{tors} 有限.

3.d. 证明, 如果 $x=z+2y$, 则 $\hat{h}(y)\leqslant\frac{1}{2}(\hat{h}(x)+\hat{h}(z))$.

3.e. 证明, 如果 Γ 为 mod 2 有限型, 则其为有限型.

II

前面已设 C 是方程 $y^2=x^3-D^2x$ 的解 $(x,y)\in\mathbf{R}^2$ 的集合. (作个 C 的草图颇有好处.) 如果 $(x_0,y_0)\in C$, 那么 C 在 (x_0,y_0) 的切线方程是 $2y_0(y-y_0)=(3x_0^2-D^2)(x-x_0)$.

如果 $(u,v)\in\mathbf{R}^*\times\mathbf{R}$, 以 (u',v') 为 $u'=\frac{1}{u}, v'=-\frac{v}{u}$ 定义的偶对, 而 $P_{u,v}$ 和 $Q_{u',v'}$ 为由

$$P_{u,v}(x)=x^3-D^2x-(ux+v)^2 \quad 和 \quad Q_{u',v'}(y)=(u'y+v')^3-D^2(u'y+v')-y^2$$

定义的多项式. 以 $D_{u,v}$ 记方程为 $y=ux+v$ 的直线. 我们可以利用以下不加证明的等价关系 (I1) $\Leftrightarrow$ (I2) $\Leftrightarrow$ (I3), 其中

(I1) $(x,y)\in D_{u,v}\cap C$,

(I2) $x>0, P_{u,v}(x)=0$ 和 $y=ux+v$,

(I3) $Q_{u'.v'}(y)=0$ 和 $x=u'y+v'>0$, 并且, 如果 $(x_0,y_0)\in C\cap D_{u,v}$, 则有等价关系 (T1) $\Leftrightarrow$ (T2) $\Leftrightarrow$ (T3), 其中

(T1) $D_{u,v}$ 在 (x_0,y_0) 切于 C,

(T2) $P_{u,v}$ 在 x_0 有个二重零点,

(T3) $Q_{u',v'}$ 在 y_0 有个二重零点.

1. 设 $n(u,v)$ 是 C 与方程为 $y=ux+v$ 的直线 $D_{u,v}$ 的相交集的基数.

1.a. 证明 $n(u,v)\leqslant 3$.

1.b. 证明 $U=\{(u,v)\in R^*\times\mathbf{R}, n(u.v)=3\}$ 是 $\mathbf{R}^2$ 的一个开集.

1.c. 证明, 如果 $n(u,v)\geqslant 2$ 且 $D_{u,v}$ 不与 C 相切, 则 $n(u,v)=3$.

1.d. 证明, 如果 $(a,b)\in\mathbf{R}^2$, 则只存在 C 的有限个点 P 使得 C 在 P 切线通过 (a,b).

2. 如果 $P=(x,y)\in C$, 则令 $x(P)=x, y(P)=y$.

2.a. 证明, 如果 $t\in\mathbf{R}$, 则在 C 上存在唯一的点 $P(t)$ 满足 $y(P(t))=t$, 并且, 如果令 $F(t)=x(P(t))$, 则 C 是点 $(F(y),y), y\in\mathbf{R}$ 的集合.

2.b. 证明对于任意的 $y\in\mathbf{R}$ 有 $F(y)\geqslant D$, F 是个偶函数, 而且 $F(y_1)=F(y_2)$ 当且仅当 $y_1=\pm y_2$ 以及 F 属于 $\mathbf{R}$ 上的 $\mathscr{C}^1$ 类.

2.c. 证明 $|y|^{-2/3}F(y)$ 当 y 趋向 $+\infty$ 或 $-\infty$ 时趋向 1.

2.d. 设 $a\in\mathbf{R}^*, t\in\mathbf{R}-\{0,a,-a\}$. 以 $D(a,t)$ 记联结从 $P(t)$ 到 $P(a)$ 的直线, 而 $H_a(t)$ 代表 $\mathbf{R}$ 中由

$$atH_a(t)=-\left(\frac{t-a}{F(t)-F(a)}\right)^3\left[\left(\frac{tF(a)-aF(t)}{t-a}\right)^3-D^2\frac{tF(a)-aF(t)}{1-a}\right]$$

定义的元. 证明我们有以下的等价关系:

[629] (i) $H_a(t)\notin\{a,t\}\Leftrightarrow P(H_a(t))$ 是 C 与 $D(a,t)$ 的第三个交点;

(ii) $H_a(t)=a\Leftrightarrow D(a,t)$ 是 C 在 $P(a)$ 的切线;

(iii) $H_a(t)=t\Leftrightarrow D(a,t)$ 是 C 在 $P(t)$ 的切线.

2.e. 计算当 t 趋向 $+\infty$ 时 $H_a(t)$ 的极限. 这时直线变成了什么?

3. 从 **2.b** 和 **2.c** 我们得到了积分 $\int_{-\infty}^{+\infty}\frac{2dt}{3F(t)^2-D^2}$ 的绝对收敛性. 以 Ω 记积分 $\int_{-\infty}^{+\infty}\frac{2dt}{3F(t)^2-D^2}$ 的值, 并定义函数 $y\mapsto L(y)$ 为

$$\int_{-\infty}^{y}\frac{2dt}{3F(t)^2-D^2}.$$

3.a. 证明 L 诱导了从 $\mathbf{R}$ 到 $]0,\Omega[$ 的双射.

3.b. 计算 $L(y)+L(-y)$, 其中 $y\in\mathbf{R}$.

4. 设 $x_1,\ldots,x_n$ 是两两不同的复数.

4.a. 证明, 如果 $Q \in \mathbf{C}[X]$ 的次数 $\leqslant n-1$, 则

$$Q(X) = \sum_{i=1}^{n} Q(x_i)(\prod_{j \neq i} \frac{X - x_j}{x_i - x_j}).$$

4.b. 证明, 如果 $P(X) = \prod_{i=1}^{n}(X - x_i)$, 且 $k \in \{0, \ldots, n-2\}$, 则 $\sum_{i=1}^{n} \frac{x_i^k}{P'(x_i)} = 0$ (其中约定 $0^0 = 1$), 并计算 $\sum_{i=1}^{n} \frac{x_i^{n-1}}{P'(x_i)}$.

5.

5.a. 设 I 为 $\mathbf{R}$ 的一个开区间, 而 $t \mapsto y_1(t), t \mapsto y_2(t), t \mapsto y_3(t)$ 是从 I 到 $\mathbf{R}$ 的 $\mathscr{C}^1$ 类函数, 使得对于任意的 $t \in I$, 点 $P_i(t) = (x_i(t), y_i(t)) = P(y_i(t)), i \in \{1, 2, 3\}$ 两两互不相同并共线. 证明函数

$$t \mapsto G(t) = L(y_1(t)) + L(y_2(t)) + L(y_3(t))$$

在 I 上为常值. (引进包含 $P_i(t)$ 的直线 $y = u(t)x + v(t)$, 并先证明 u 和 v 在 I 属于 $\mathscr{C}^1$.)

5.b. 证明, 如果 $H_a(t)$ 是在问题 **2.d** 中引进的那个函数, 那么对于所有的 $a > 0$ 和 $t > a$ 有 $L(a) + L(t) + L(H_a(t)) = 2\Omega$.

5.c. 证明, 如果 y_1, y_2, y_3 是 $\mathbf{R}$ 中的三个两两互不相同的数, 使得 $P(y_1), P(y_2)$ 和 $P(y_3)$ 共线, 那么 $L(y_1) + L(y_2) + L(y_3) \in \{\Omega, 2\Omega\}$.

5.d. 证明, 如果 $y_1 \neq y_2$, 而 $P(y_2)$ 位于 C 在 $P(y_1)$ 的切线上, 则 $2L(y_1) + L(y_2)$ 属于 $\{\Omega, 2\Omega\}$.

5.e. 证明, 如果 y_1, y_2, y_3 是 $\mathbf{R}$ 中的三个两两互不相同的数, 使得 $L(y_1) + L(y_2) + L(y_3) \in \Omega\mathbf{Z}$, 则 $P(y_1), P(y_2)$ 和 $P(y_3)$ 共线.

6. 如果 G 是模为 1 的复群, 并设 $E : \bar{\mathbf{C}} \to G$ 的定义为: $E(\infty) = 1$ 而对于 $y \in \mathbf{R}$ 有 $E(P(y)) = \exp(\frac{2i\pi}{\Omega} L(y))$.

6.a. 证明在 $\bar{\mathbf{C}}$ 上存在唯一的交换群的运算 $+$, 使得我们有 $E(P + Q) = E(P)E(Q)$. 又证明, 如果 $P + Q \neq \infty$, 则当 $L(y(P)) + L(y(Q)) < \Omega$ 时有 $L(y(P + Q)) = L(y(Q)) + L(y(Q))$, 而当 $L(y(P)) + L(y(Q)) > \Omega$ 时有 $L(y(P+Q)) = L(y(P)) + L(y(Q)) - \Omega$.

6.b. 证明 ∞ 是对于 $+$ 的中性元, 而若 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ 和 $P_3 = (x_3, y_3)$ 是 C 的三个不同元, 则 $P_1 + P_2 + P_3 = \infty$ 当且仅当 P_1, P_2 和 P_3 共线. [630]

6.c. 证明, 如果 $P \in C$, 则 P 对于 $+$ 的逆元 $-P$ 为 P 相对于 x 轴的对称点.

6.d. 证明, 如果 $P \in \bar{\mathbf{C}}$, 则方程 $2Q = P$ 总有解; 有多少个?

6.e. 证明, 如果 $y_1 + y_2 \neq 0$, 而 z_1 趋向 y_1, z_2 趋向 y_2, 则 $y(P(z_1) + P(z_2)$ 趋向 $y(P(y_1) + P(y_2))$. 当 $y_1 + y_2 = 0$ 时情形如何?

III

在问题 **1.b, 2.b** 和 **4.** 中, 我们想要建立群的一些公式. 在每个群中, 我们将证明那些不在方括号中的公式, 而不证明在方括号中的.

1. 设 $P_1=(x_1,x_2), P_2=(x_2,y_2)$ 为 C 的两个元, 其中 $x_1\neq x_2$, 且 $P_3=(x_3,y_3)\in C$ 由 $P_1+P_2+P_3=\infty$ 定义.

1.a. 证明 x_1,x_2,x_3 为多项式

$$P(x)=x^3-D^2x-\left(y_1+\frac{y_2-y_1}{x_2-x_1}(x-x_1)\right)^2$$

的根. 由此推出有

$$x_3=\left(\frac{x_1^2+x_1x_2+x_2^2-D^2}{y_1+y_2}\right)^2-x_1-x_2 \quad \text{和} \quad y_3=\frac{x_1^2+x_1x_2+x_2^2-D^2}{y_1+y_2}(x_3-x_1)+y_1.$$

(首先假设 P_1,P_2 和 P_3 互不相同.)

1.b. 建立公式 (承认方括号里的公式而无需证明)

$$(x_1+D)(x_2+D)(x_3+D)=\left(\frac{(x_1+D)y_2-(x_2+D)y_1}{x_2-x_1}\right)$$

$$\left[x_1x_2x_3=\left(\frac{x_1y_2-x_2y_1}{x_2-x_1}\right)^2\right].$$

2. 设 $P=(x,y)\in C$, 其中 $y\neq 0$, 并设 $2P=(x',y')$.

2.a. 建立公式:

$$x'=\left(\frac{3x^2-D^2}{2y}\right)^2-2x \quad \text{和} \quad -y'=\frac{3x^2-D^2}{2y}(x'-x)+y.$$

2.b. 证明 $x'=(\frac{x^2+D^2}{2y})^2$. 同样, 我们承认

$$\left[x'+D=\left(\frac{x^2+2Dx-D^2}{2y}\right)^2 \quad \text{和} \quad x'-D=\left(\frac{x^2-2Dx-D^2}{2y}\right)^2\right].$$

3. 证明 $\bar{C}(\mathbf{Q})$ 是 $\bar{C}$ 的子群.

4. 设 $P_1=(x_1,y_1), P_2=(x_2,y_2)$ 为 $C(\mathbf{Q})$ 的两个元, 满足 $x_1\neq x_2$, 并设 $P_3=P_1+P_2=(x_3,y_3)$, 而 $P_4=P_1-P_2=(x_4,y_4)$. 建立以下公式 (对于方括号中的公式承认而无需证明):

$$(x_3+D)(x_4+D)=\left(\frac{x_1x_2+D(x_1+x_2)-D^2}{x_2-x_1}\right)^2 \quad \text{和} \quad \left[x_3x_4=\left(\frac{x_1x_2+D^2}{x_2-x_1}\right)^2\right].$$

IV

[631]

IV.A

1. 如果 p 是个素数而 $a \in \mathbf{Z} - \{0\}$, 那么定义整数 $v_p(a)$ 为使得 p^n 整除 a 的最大的整数 n(譬如, $48 = 3 \cdot 2^4$, 于是 $v_2(48) = 4, v_3(48) = 1$, 而对素数 $p \notin \{2,3\}$ 有 $v_p(48) = 0$). 我们有 $v_p(ab) = v_p(a) + v_p(b)$, 那么可将 v_p 延拓到 $\mathbf{Q}^*$ 上: $v_p(ab^{-1}) = v_p(a) - v_p(b)$. 如果 $a \in \mathbf{Q}^*$, 则除了有限个素数 p 外都有 $v_p(a) = 0$, 并且, 如果 a 为正, 则 $a = \prod_p p^{v_p(a)}$. 如果 $v \in \mathbf{Z}$, 以 $\bar{v}$ 记其在 $\mathbf{Z}/2\mathbf{Z}$ 中的像.

1.a. 证明 $a \in \mathbf{Q}^*$ 是一个平方数当且仅当 $a > 0$ 且对于所有的素数 p 有 $\overline{v_p(a)} = 0$.

1.b. 证明, 如果 $a, b \in \mathbf{Q}^*$ 满足 $v_p(a) < v_p(b)$, 则 $v_p(a+b) = v_p(a)$.

2. 设 $P = (x,y) \in C(\mathbf{Q})$, 且 $c \in \{1,4,9,16,\ldots\}$ 是使得 $a = cx \in \mathbf{Z}$ 的最小平方整数.

2.a. 证明, 如果 $v_p(c) \geqslant 1$, 则 $v_p(c) \geqslant 2$ 且 $v_p(a) \in \{0,1\}$.

2.b. 证明 $a(a-Dc)(a+Dc)$ 是个平方数.

2.c. 证明, 如果 $p \notin S \cup \{2\}$, 则 $v_p(a)$ 和 $v_p(a+Dc)$ 都为偶数.

3. 设 $\varphi : \bar{C}(\mathbf{Q}) \to (\mathbf{Z}/2\mathbf{Z})^{2s+2}$ 将 ∞ 映到 $(0,\ldots,0)$, 而将 $P = (x,y)$ 映到

$$(\overline{v_2(x)}, \overline{v_{p_1}(x)}, \ldots, \overline{v_{p_s}(x)}, \overline{v_2(x+D)}, \overline{v_{p_1}(x+D)}, \ldots, \overline{v_{p_s}(x+D)})$$

的映射.

3.a. 证明 φ 是从 $\bar{C}(\mathbf{Q})$ 到 $(\mathbf{Z}/2\mathbf{Z})^{2s+2}$ 的一个群态射.

3.b. 证明, 如果 $P = (x', y') \in C(\mathbf{Q})$ 是使得 $x', x' - D$ 和 $x' + D$ 为 $\mathbf{Q}$ 中的平方数, 并且如果 $Q \in C$ 是方程 $2Q = P$ 的解, 则 $Q \in C(\mathbf{Q})$.

3.c. 对 φ 的核做特征描述.

3.d. 证明 $\bar{C}(\mathbf{Q})$ 为 mod 2 的有限型.

IV.B

定义一个函数 $h : \bar{C}(\mathbf{Q}) \to \mathbf{R}_+$, 它将 ∞ 映到 0, 而将 $P = (x,y)$ 映到 $\log(a + Dc) = \log(c(x+D))$, 其中 c 是使得 $a = cx$ 为整数的最小的平方整数.

1. 证明, 对任意的 $P \in \bar{C}(\mathbf{Q})$ 有

$$h(2P) \leqslant 4h(P).$$

2. 设 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ 为 $C(\mathbf{Q})$ 中的两个元, 其中 $x_1 \neq x_2$, 并设 $P_3 = P_1 + P_2 = (x_3, y_3), P_4 = P_1 - P_2 = (x_4, y_4)$. 又设 c_1(分别地, c_2) 是使 $a_1 = c_1 x_1$(分别地, $a_2 = c_2 x_2$) 为整数的最小的平方整数.

2.a. 证明, 如果 d 整除 $T = a_1a_2 + D^2c_1c_2, U = a_1a_2 - D^2c_1c_2 + D(a_1c_2 + a_2c_1)$ 和 $V = a_1c_2 - a_2c_1$, 则 d 也整除 $2a_1(a_2 + Dc_2)$ 和 $2a_2(a_1 + Dc_1)$, 也同样整除 $4D^2a_1c_2^2$ 和 $4D^2a_2c_1^2$.

2.b. 证明, 如果 $p \notin S \cup \{2\}$, 则 p 不整除 $4D^2a_1c_2^2, 4D^2a_2c_1^2$ 或 $a_1a_2 + D^2c_1c_2$ (先证明 p 既不整除 a_1 和 c_1 的最大公因子, 也不整除 a_2 和 c_2 的最大公因子).

2.c. 证明, 如果 $p \in S \cup \{2\}$, 则 p^4 不整除 $4D^2a_1c_2^2, 4D^2a_2c_1^2$ 或 $a_1a_2 + D^2c_1c_2$.

2.d. 证明 $a_1a_2 + D^2c_1c_2, a_1a_2 - D^2c_1c_2 + D(a_1c_2 + a_2c_1)$ 和 $a_1c_2 - a_2c_1$ 的最大公因子整除 $(2D)^3$.

[632] **2.e.** 证明, 如果 $x_3x_4 = \frac{d}{e}$ 和 $(x_3 + D)(x_4 + D) = \frac{d'}{e}$, 其中 d, d' 和 e 是整数, 又若 c_3 (分别地, c_4) 是使 $a_3 = c_3x_3$ (分别地, $a_4 = c_4x_4$) 为整数的最小的平方整数, 且若 $\delta = \gcd(d, d', e)$, 则 $\frac{c_3c_4\delta}{e}$ 是整数, 并且 $h(P_3) + h(P_4) \geqslant \log d' - \log \delta$.

2.f. 证明对于任意的 $(P_1, P_2) \in C(\mathbf{Q})^2, P_1 \pm P_2 \neq \infty$, 我们有

$$h(P_1 + P_2) + h(P_1 - P_2) \geqslant 2(h(P_1) + h(P_2)) - \log(32D^3).$$

3. 现在假设 $\bar{C}(\mathbf{Q})$ 为无限群.

3.a. 证明方程 $2P = \infty$ 仅有的解为 $P = \infty$ 和 $P = (D, 0)$.

3.b. 证明对任意的 $P \in \bar{C}(\mathbf{Q})$ 有 $h(2P) \geqslant 4h(P) - 6\log(2(2D)^3)$.

3.c. 证明存在 $A > 0$ 使得对任意的 $(P, Q) \in \bar{C}(\mathbf{Q})^2$ 有

$$h(P + Q) + h(P - Q) \geqslant 2(h(P) + h(Q)) - A.$$

3.d. 证明 h 是 $\bar{C}(\mathbf{Q})$ 上的一个高.

3.e. 证明 h 是 $\bar{C}(\mathbf{Q})$ 上的容许高.

3.f. 证明 $\bar{C}(\mathbf{Q})_{\text{tors}}$ 是个有限群而 $\bar{C}(\mathbf{Q})$ 为有限型.

问题校正

I

1.a. 如果 $nx = 0, my = 0$, 则 $nm(x - y) = mnx - nmy = 0$.

1.b. 否: 例如, 如果 $\Gamma = \mathbf{C}^*$, 则 Γ_{tors} 是任意阶的单位根的集合, 因而无限.

2.a. 令 $x_n = 4^{-n}h(2^nx), M_0 = M + h(0)$. 我们有 $|h(2^{n+1}x) + h(0) - 4h(2^nx)| \leqslant M$, 从而 $|x_{n+1} - x_n| \leqslant \frac{M_0}{4^{n+1}}$. 因此有 $|x_{n+k} - x_n| \leqslant \sum_{i=1}^{k} \frac{M_0}{4^{n+i}} \leqslant \sum_{i=1}^{+\infty} \frac{M_0}{4^{n+i}} = \frac{M_0}{3 \cdot 4^n}$, 其中 $(n, k) \in \mathbf{N}^2$.

2.b. $|\frac{h(2^n(x+y))}{4^n} + \frac{h(2^n(x-y))}{4^n} - 2\frac{h(2^nx)}{4^n} - 2\frac{h(2^ny)}{4^n}| \leqslant \frac{M}{4^n}$, 取极限便得到结果.

2.c. 我们对 $n \geqslant 0$ 来归纳证明当 $0 \leqslant k \leqslant n$ 时有 $\hat{h}(kx) = k^2\hat{h}(x)$. 取 $x = y = 0$ 得到 $2\hat{h}(0) = 4\hat{h}(0)$, 从而 $\hat{h}(0) = 0$, 于是此性质对于 $n = 0$ 和 $n = 1$ 为真. 至于从 n

到 $n+1$, 只要注意

$$\hat{h}((n+1)x) = 2\hat{h}(nx) + 2\hat{h}(x) - \hat{h}((n-1)x) = (2n^2+2-(n-1)^2)\hat{h}(x) = (n+1)^2\hat{h}(x).$$

因此此性质对于所有 $n \geqslant 0$ 为真. 另外, 取 $x=0, y=a$ 则得到 $\hat{h}(a)+\hat{h}(-a) = 2\hat{h}(a)$, 从而 $\hat{h}(-a) = \hat{h}(a)$, 因而 $\hat{h}$ 为偶函数. 因此函数 $n \mapsto \hat{h}(nx) - n^2\hat{h}(x)$ 是 $n \in \mathbf{Z}$ 的偶函数并对 $n \in \mathbf{Z}$ 为零; 故恒等于零.

3.a. 取极限有 $\hat{h}(x) \geqslant 0$, 并由问题 **2.b** 知它是个高; 又根据问题 **2.a** 知 $\hat{h}(x) \leqslant B$ 意味着 $h(x) \leqslant B + M'$, 故 $\hat{h}$ 是个容许高.

3.b. 如果 $mx = 0$, 则 $\hat{h}(mx) = m^2\hat{h}(x)$, 从而 $\hat{h}(x) = 0$.

反之, 如果 $\hat{h}(x) = 0$, 于是根据问题 **2.c.**, 对于与任意的 $n \in \mathbf{Z}$ 有 $\hat{h}(nx) = 0$, 但由于 $\hat{h}$ 是容许高, 故集合 $\{nx, n \in \mathbf{Z}\}$ 有限, 因此存在 $n_1 \neq n_2$ 使得 $n_1x = n_2x$, 于是 $(n_1 - n_2)x = 0$, 故 $x \in \Gamma_{\text{tors}}$.

3.c. 这是前一个问题和 $\hat{h}$ 的容许性的直接结果.

3.d. 由于 $\hat{h}(x+z) \geqslant 0$, 故有 $4\hat{h}(y) = \hat{h}(2y) = \hat{h}(x-z) \leqslant 2\hat{h}(x) + 2\hat{h}(z)$.

3.e. 由假设条件, 存在一个有限集 Z 使得 Γ 的所有元 x 可以写为 $x = z + 2y$ 的形式, 其中 $z \in Z, y \in \Gamma$. 设 $B = \sup_{z \in Z} \hat{h}(x)$, $A = \{a \in \Gamma, \hat{h}(a) \leqslant 2B\}$. 于是 A 是有限集; 以 $a_1, \ldots, a_r$ 记其元. 我们对 k 来归纳证明 Γ 中所有满足 $\hat{h}(x) \leqslant (2^k+1)B$ 的元 x 可以写为 $n_1a_1 + \cdots + n_ra_r$ 的形式. 对于 $k=0$ 由构造知其为真. 如果 $k \in \mathbf{N}$ 且 $\hat{h}(x) \leqslant (2^{k+1}+1)B$, 则可将 x 写成 $x = z + 2y$ 的形式, 其中 $z \in Z, y \in \Gamma$, 满足 $\hat{h}(y) \leqslant \frac{1}{2}(\hat{h}(z) + \hat{h}(x)) \leqslant \frac{1}{2}(B + (2^{k+1}+1)B) = (2^k+1)B$, 这让我们可以利用对于 y 的归纳假定, 那么注意到 $z \in Z \subset A$, 便得结论. [633]

II

1.a. $D_{u,v} \cap C$ 与三次多项式 $P_{u,v}$ 的根的集合有一个双射.

1.b. 设 $(a,b) \in \mathbf{R}^* \times \mathbf{R}$ 满足 $n(a,b) = 3$. 于是多项式 $P_{a,b}$ 有三个实的单根 $0 < x_1 < x_2 < x_3$, 并由于 $P_{a,b}$ 在 $-\infty$ 的邻域中 < 0, 故有 $P_{a,b}(0) < 0, P_{a,b}(\frac{x_1+x_2}{2}) > 0$ 以及 $P_{a,b}(\frac{x_2+x_3}{2}) < 0$. 由连续性, 存在包含 (a,b) 的一个开集 $U_{a,b}$ 使得当 $(u,v) \in U_{a,b}$ 时有 $P_{u,v}(0) < 0, P_{u,v}(\frac{x_1+x_2}{2}) > 0$ 和 $P_{u,v}(\frac{x_2+x_3}{2}) < 0$, 这表明 $P_{u,v}$ 在 0 与 $\frac{x_1+x_2}{2}$ 之间, 在 $\frac{x_1+x_2}{2}$ 与 $\frac{x_2+x_3}{2}$ 之间以及 $\frac{x_2+x_3}{2}$ 与 $+\infty$ 之间都有零点, 因此 $n(u,v) = 3$. 这便证明了 $U \supset U_{a,b}$, 得证.

1.c. 如果 $n(u,v) \geqslant 2$, 且若 $D_{u,v}$ 不切于 C, 那么多项式 $P_{u,v}$ 有三个不同的实根, 其中两个 > 0. $P_{u,v}$ 的常数项为 $-v^2$ 且自然可分成两种情形.

— $v = 0$, 于是 $P_{u,v}$ 的两个非零根的乘积等于 $-D^2 < 0$, 它与这两个根均 > 0 矛盾. 从而在这种情形下得到结论.

— $v \neq 0$, 于是 $P_{u,v}$ 的根的乘积 $v^2 > 0$, 它表明 $P_{u,v}$ 的第三个根 > 0 从而 $n(u,v) = 3$.

1.d. 属于 C 并使得 (a,b) 属于 C 在 $P=(x,y)$ 的切线上的这些点 P 的集合就是满足方程 $y^2=x^3-D^2x, x>0$ 和 $2y(b-y)=(3x^2-D^2)(a-x)$ 的偶对 $(x,y)\in\mathbf{R}^2$ 的集合. 特别地, $2by=(3x^2-D^2)(a-x)+2y^2=2x^3+3ax^2+3D^2x-D^2a$. 如果 $b=0$, 则 x 是一个 3 次多项式的根并由于对于每个 x 的值有 $y^2=x^3-D^2x$, 故最多只有 2 个 y 的值, 这让我们得知它最多只有 6 个解 (x,y). 如果 $b\neq 0$, 对于方程 $y^2=x^3-Dx$ 中的 y 的值, 由于我们知道 x 是一个 6 次多项式的根, 因此最多只有 12 对解 (x,y).

2.a. 如果 $t\in\mathbf{R}$, 函数 $x\mapsto x^3-D^2x-t^2$ 从 0 到 $\frac{D}{\sqrt{3}}$ 递降, 而从 $\frac{D}{\sqrt{3}}$ 到 $+\infty$ 递增. 由于在 $x=0, x=D$ 它 $\leqslant 0$, 故在 $]0,D[$ 上不取零, 又由于它在 $+\infty$ 趋向 $+\infty$, 故它在 $[D,+\infty[$ 取零且只取零一次. 如果以 $F(t)$ 记它在那里取零的点, 则 $(F(t),t)$ 是在 C 上满足 $y(P(t))=t$ 的唯一的点, 断言得证.

2.b. 函数 $x\mapsto x^3-D^2x$ 在 $]\frac{D}{\sqrt{3}},+\infty[$ 上递增且属于 $\mathscr{C}^1$; 因此是从 $]\frac{D}{\sqrt{3}},+\infty[$ 到 $]-\frac{2D^3}{3\sqrt{3}},+\infty[$ 的双射, 其逆 G 也属于 $\mathscr{C}^1$ 类并满足 $G(0)=D$; 由于有 $F(t)=G(t^2)$, 故得结论.

2.c. 如果 $y\in\mathbf{R}$, 令 $f_y(x)=x^3-D^2x-y^2$. 设 $\varepsilon>0$. 于是 $f_y((1+\varepsilon)|y|^{2/3})$ 和 $f_y((1-\varepsilon)|y|^{2/3})$ 在 $|y|=+\infty$ 的邻域中分别等价于 $((1+\varepsilon)^3-1)y^2$ 和 $((1-\varepsilon)^3-1)y^2$. 特别地, 如果 $|y|$ 充分大, 则 $f_y((1+\varepsilon)|y|^{2/3})$ 和 $f_y((1-\varepsilon)|y|^{2/3})$ 具有相反的符号, 从而 $(1-\varepsilon)|y|^{2/3}\leqslant F(y)\leqslant(1+\varepsilon)|y|^{2/3}$. 由此得到, 当 $|y|$ 趋向 $+\infty$ 时 $|y|^{-2/3}F(y)$ 趋向 1.

2.d. 直线 $D(a,t)$ 的方程是 $x-F(a)=\frac{F(t)-F(a)}{t-a}(y-a)$, 将其重写为 $x=\frac{F(t)-F(a)}{t-a}y+\frac{F(a)t-aF(t)}{t-a}$ 的形式. 为了了解 $D(a,t)$ 与 C 的交, 我们利用等价关系 (I1) $\Leftrightarrow$ (I3) 并考虑多项式 $Q_{u,v}$, 其中 $u=\frac{F(t)-F(a)}{t-a}$ 而 $v=\frac{F(a)t-aF(t)}{t-a}$, 其首项系数是 u^3, 常数项是 v^3-D^2v. $Q_{u,v}$ 的根的乘积因而是 $-\frac{v^3-D^2v}{u^3}$, 并由构造知 $Q_{u,v}$ 有根 a 和 t, 而它的第三个根便是 $-\frac{v^3-D^2v}{atu^3}=H_a(t)$. 所要证明的这些结果因而是问题 **1.c** 和等价关系 (T1) $\Leftrightarrow$ (T3) 的直接推论. [634]

2.e. 由于在 $+\infty$ 的邻域中 $F(t)\sim t^{2/3}$, 故当 t 趋向 $+\infty$ 时有 $\frac{1}{t}(\frac{t-a}{F(t)-F(a)})^3$ 趋向 1, 而 $H_a(t)$ 趋向 $-\frac{1}{a}(F(a)^3-D^2F(a))=-\frac{1}{a}\cdot a^2=-a$, 并且直线 $D(t,a)$ 变为竖直的.

3.a. 我们有 $L'(y)=\frac{2}{3F(y)^2-D^2}>0$, 它证明了 L 是一个从 $\mathbf{R}$ 到其上的一个递增双射. 由于 $\lim_{y\to-\infty}L(y)=0$ 和 $\lim_{y\to+\infty}L(y)=\Omega$, 故有结论.

3.b. 由于 F 是个偶函数, 故有 $L(-y)=\int_{-\infty}^{-y}\frac{2}{3F(t)^2-D^2}dt=\int_{y}^{+\infty}\frac{2}{3F(t)^2-D^2}dt$, 故 $L(-y)+L(y)=\int_{-\infty}^{+\infty}\frac{2}{3F(t)^2-D^2}dt=\Omega$.

4.a. 两端都是次数 $\leqslant n-1$ 的多项式, 并在 $x_1,\ldots,x_n$ 取相同的值. 那么它们的差是一个次数 $\leqslant n-1$ 的多项式, 但具有 n 个根, 故为零.

4.b. 如果将前面的结果用于 X^k, 并使它们的 $n-1$ 次的项恒同, 再注意到 $\prod_{j\neq i}(x_i-x_j)=P'(x_j)$, 便得到: 当 $k\leqslant n-2$ 时 $\sum_{i=1}^{n}\frac{x_i^k}{P'(x_i)}=0$, 而当 $k=n-1$ 时

有 $\sum_{i=1}^{n} \frac{x_i^k}{P'(x_i)} = 1$.

5.a. 因为 y_1, y_2 和 F 属于 $\mathscr{C}^1$, 同时又由于 $y_1(t) \neq y_2(t)$ 且 > 0 (因而 $y_1(t) \neq \pm y_2(t)$), 故 $F(y_1(t)) - F(y_2(t))$ 不为零, 因此 $u(t) = \frac{y_2(t)-y_1(t)}{F(y_2(t))-F(y_1(t))}$ 和 $v(t) = y_1(t) - \frac{y_2(t)-y_1(t)}{F(y_2(t))-F(y_1(t))} F(y_1(t))$ 也属于 $\mathscr{C}^1$. 我们有 $\frac{1}{2}G' = \sum_{i=1}^{3} \frac{y_i'}{3x_i^2 - D^2}$. 另外, 也有

$$2y_i y_i' = (3x_i^2 - D^2)x_i' \quad 和 \quad y_i' = ux_i' + u'x_i + v'.$$

可以在这两个方程中消去 x_i' 从而得到

$$(3x_i^2 - D^2 - 2uy_i)y_i' = (3x_i^2 - D^2)(u'x_i + v')$$

和

$$\frac{1}{2}G' = u' \sum_{i=1}^{3} \frac{x_i}{3x_i^2 - D^2 - 2uy_i} + v' \sum_{i=1}^{3} \frac{1}{3x_i^2 - D^2 - 2uy_i}.$$

又, x_1, x_2, x_3 是形式 $P(x) = x^3 - D^2x - (ux+v)^2$ 的根, 而它的导数是 $3x^2 - D^2 - 2u(ux+v)$, 并由于 $y_i = ux_i + v$, 故由前面的方程得到 $\frac{1}{2}G' = u' \sum_{i=1}^{3} \frac{x_i}{P'(x_i)} + v' \sum_{i=1}^{3} \frac{1}{P'(x_i)} = 0$. 因此 G 在 I 上的导数恒为零, 因而它为常数.

5.b. 给出的 $H_a(t)$ 的公式证明了函数 $H_a(t)$ 属于 $\mathscr{C}^1$. 前面的这个问题因而证明了 $G(t) = L(a) + L(t) + L(H_a(t))$ 在每个 I 上为常值, 其中 I 是对于所有 $t \in I$ 有 $H_a(t) \notin \{a, t\}$ 的区间. 另外, 使得 $H_a(t) = a$ 的 t 的集合为有限的 (它是 C 在 $P(a)$ 的切线与 C 的交集), 同样地, 根据问题 **1.d.**, $H_a(t) = t$ 的 t 的集合也是有限的. 因此那些对于任意 $t \in I$ 使得 $H_a(t) \notin \{a, t\}$ 的区间 I 的并, 除了可能的有限个点外, 覆盖了 $]a, +\infty[$, 而由于 G 在每个这样的区间上为常值并在 $]a, +\infty[$ 上连续, 故它在 $]a, +\infty[$ 上为常值. 于是, 根据问题 **2.e** 和 **3.b** 有 $G(+\infty) = \lim_{t\to+\infty} G(t) = L(a) + L(-a) + \lim_{t\to+\infty} L(t) = 2\Omega$.

5.c. 如果在 y_1, y_2, y_3 中有两个 > 0, 那么前面的问题便证明了 $L(y_1) + L(y_2) + L(y_3) = 2\Omega$. 如果其中有两个 < 0, 则 $L(y_1) + L(y_2) + L(y_3) = 3\Omega - (L(-y_1) + L(-y_2) + L(-y_3)) = \Omega$. $y_1 = 0, y_2 > 0, y_3 < 0$ 的情形是不可能出现的, 否则, 因为 $y_1 = 0$ 意味着 $x_1 = D$, 并由于 $x_2, x_3 > D$, 故 $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ 便不可能共线.

5.d. 令 $a = y_2$. 由于通过 $P(a)$ 只有有限条直线与 C 相切, 故存在一个包含 y_1 的开区间 I 使得对于 $t \in I - \{y_1\}$, 直线 $D(a, t)$ 不切于 C; 但由此知 $H_a(t)$ 在 $t = y_1$ 连续, 故 $L(a) + L(t) + L(H_a(t))$ 在 $I - \{y_1\}$ 上取值于 $\{\Omega, 2\Omega\}$ 中; 所以它在 I 上为常值, 取极限便得到了 $2L(y_1) + L(y_2) \in \{\Omega, 2\Omega\}$.

5.e. 根据问题 **1.c.**, 联结 $P(y_1)$ 到 $P(y_2)$ 的直线交 C 于第三个点 $P(z)$ 或者在 $P(y_1)$(分别地, $P(y_2)$) 切于 C. 在后面的情形令 $z = y_1$(分别地, $z = y_2$). 根据问题 **5.c** 和 **5.d**, 在所有的情形中都有 $L(y_1) + L(y_2) + L(z) \in \Omega\mathbf{Z}$, 从而 $L(z) - L(y_3) \in \Omega\mathbf{Z}$. [635] 但由于 $L(z) - L(y_3) \in] - \Omega, \Omega[$, 这意味着 $L(z) - L(y_3) = 0$, 并因为 L 是个单射, 故 $z = y_3$.

6.a. 根据问题 **3.a**, E 是从 $\bar{C}$ 到 G 的一个双射从而能够 (也应该) 由公式 $P+Q=E^{-1}(E(P)E(Q))$ 定义运算 $+$. 于是应该有 $\exp(\frac{2i\pi}{\Omega}(L(y(P+Q))-L(y(P))-L(y(P))-L(y(Q))))=1$, 因此 $L(y(P+Q))-L(y(P))-L(y(Q))\in\Omega\mathbf{Z}$. 本问题的其余部分来自 $L(y(P))+L(y(Q))\in]0,2\Omega[$ 和 $L(y(P+Q))\in]0,\Omega[$.

6.b. 由构造知 $\infty=E^{-1}(1)$ 是 $+$ 的中性元, 而 $P_1+P_2+P_3=\infty$ 当且仅当 $L(y_1)+L(y_2)+L(y_3)\in\Omega\mathbf{Z}$, 根据问题 **5.c** 和 **5.e**, 这就是说, 当且仅当 P_1,P_2,P_3 共线.

6.c. 如果 $P=(x,y)$ 和 $-P=(x',y')$, 则有 $L(y)+L(y')\in\Omega\mathbf{Z}$, 并由于 $L(y)$ 和 $L(y')$ 属于 $]0,\Omega[$, 它表明 $L(y')=\Omega-L(y)=L(-y)$, 因 L 为单射, 从而 $y'=-y$.

6.d. 由于 E 诱导了从 $\bar{C}$ 到 G 的同构, 那么方程 $2Q=P$ 的解集与方程 $z^2=E(P)$ 的解集间有一个双射; 因而方程 $2Q=P$ 总有两个解.

6.e. 如果 $y_1+y_2\neq0$, 则 $L(y_1)+L(y_2)\neq\Omega$, 如有必要可将 y_1 换作 $-y_1$, y_2 换作 $-y_2$, 故不妨设 $0<L(y_1)+L(y_2)<\Omega$. 因为 L 连续, 故存在开区间 $I_1\ni y_1, I_2\ni y_2$ 使得当 $(z_1,z_2)\in I_1\times I_2$ 时有 $0<L(z_1)+L(z_2)<\Omega$. 由于此双射的逆 $L^{-1}:]0,\Omega[\to\mathbf{R}$ 连续, 故 $(z_1,z_2)\mapsto L^{-1}(L(z_1)+L(z_2))$ 是 $I_1\times I_2$ 上的连续函数. 证完.

III

1.a. 先假设 P_1,P_2,P_3 互不相同. 通过 P_1 和 P_2 的直线的方程是 $y=y_1+\frac{y_2-y_1}{x_2-x_1}(x-x_1)$. 由此推出 x_1,x_2,x_3 是多项式

$$P(x)=x^3-D^2x-\left(y_1+\frac{y_2-y_1}{x_2-x_1}(x-x_1)\right)^2$$

的根. 这个多项式的根的和从而是 $(\frac{y_2-y_1}{x_2-x_1})^2$, 并由于

$$\frac{y_2-y_1}{x_2-x_1}=\frac{y_2^2-y_1^2}{(y_1+y_2)(x_2-x_1)}=\frac{x_2^3-D^2x_2-x_1^3+D^2x_1}{(y_1+y_1)(x_2-x_1)}=\frac{x_1^2+x_1x_2+x_2^2-D^2}{y_1+y_2},$$

因此得到 $x_3=(\frac{x_1^2+x_1x_2+x_2^2-D^2}{y_1+y_2})^2-x_1-x_2$. 利用前面的公式以及 P_3 在方程为 $y=y_1+\frac{y_2-y_1}{x_2-x_1}(x-x_1)$ 的直线上的事实便得到了 y_3 的公式. $P_3\in\{P_1,P_2\}$ 的情形可由连续性从一般情形推出 (参看第 II 部分的问题 **6.e**).

1.b. x_1+D,x_2+D 和 x_3+D 是多项式 $P(x-D)$ 的根, 而此多项式的常数项为 $-(\frac{y_2-y_1}{x_2-x_1}(-D-x_1)+y_1)^2=-(\frac{y_1(x_2+D)-y_2(x_1+D)}{x_2-x_1})^2$.

2.a. 这些公式可以利用连续性从问题 **1.a** 的公式推出.

2.b. 我们有 $x'=(\frac{3x^2-D^2}{2y})^2-2x=\frac{9x^4-6D^2x^2+D^4-8xy^2}{4y^2}$, 又由于 $y^2=x^3-D^2x$, 故也有 $9x^4-6D^2x^2+D^4-8xy^2=x^4+2D^2x^2+D^4=(x^2+D^2)^2$.

3. 由于 $-P$ 是 P 相对于 x 轴的对称点, 故 $\bar{C}(\mathbf{Q})$ 在取相反元时稳定. 设 P 和 Q 属于 $\bar{C}(\mathbf{Q})$. 要证明的是 $P+Q\in\bar{C}(\mathbf{Q})$. 如果 $P=\infty$ 或 $Q=\infty$ 或 $P=-Q$, 这是显然的. 在所有其他情形, $y(P)+y(Q)\neq0$, 从而可以利用问题 **2.a** 和 **3.a** 得到结果.

4. 根据问题 **2.b**, 有 [636]

$$(x_1+D)(x_2+D)(x_3+D)=\left(\frac{(x_1+D)y_2-(x_2+D)y_1}{x_2-x_1}\right)^2,$$
$$(x_1+D)(x_2+D)(x_4+D)=\left(\frac{(x_1+D)y_2+(x_2+D)y_1}{x_2-x_1}\right)^2,$$

从而 $(x_3+D)(x_4+D)$ 是 $\frac{(x_1+D)^2y_2^2-(x_2+D)^2y_1^2}{(x_1+D)(x_2+D)(x_1-x_2)^2}$ 的平方. 由于 $y_i^2=x_i^3-D^2x_i=x_i(x_i+D)(x_i-D)$, 这表明 $(x_3+D)(x_4+D)$ 也是下面表达式的平方:

$$\frac{(x_1+D)x_2(x_2-D)-(x_2+D)x_1(x_1-D)}{(x_1-x_2)^2}=\frac{x_1x_2+D(x_1+x_2)-D^2}{x_2-x_1}.$$

IV.A

1.a. 如果 $b\in\mathbf{Q}^*$ 且 $a=b^2$, 于是 $a>0$ 并且 $v_p(a)=2v_p(b)$ 被 2 整除. 反之, 如果 $a>0$ 且 $v_p(a)=2n_p$, 则 a 是 $\prod_p p^{n_p}$(其为有限积) 的平方.

1.b. 我们有 $v_p(da)=v_p(a)+v_p(d)$ 和 $v_p(d(a+b))=v_p(a+b)+v_p(d)$, 于是取 d 为 a 和 b 的分母的乘积时便化成了 a 和 b 为整数的情形. 令 $a=p^{v_p(a)}a'$, $b=p^{v_p(a)}p^{v_p(b)-v_p(a)}b'$, 其中 a',b' 与 p 互素. 由于 $v_p(b)-v_p(a)>0$, 故 p 整除 $p^{v_p(b)-v_p(a)}b'$, 而由于 a' 与 p 互素, 于是 p 不整除 $c=a'+p^{v_p(b)-v_p(a)}b'$, 从而 $a+b=p^{v_p(a)}c$ 满足 $v_p(a+b)=v_p(a)$.

2.a. 由于 c 是个平方数, 故 $v_p(c)$ 是个整数, 而 $v_p(c)\geqslant 1$ 表明 $v_p(c)\geqslant 2$. 另一方面, a 不被 p^2 整除, 否则 $(p^{-2}c)a$ 就会是整数, 这与 c 的最小性矛盾; 因此 $v_p(a)\leqslant 1$, 从而 $v_p(a)\in\{0,1\}$.

2.b. 我们有 $a(a-Dc)(a+Dc)=c^3y^2$, 并由于 c 是个平方数, 故由此知 $a(a-Dc)(a+Dc)$ 同样是个平方数.

2.c. 设 p 是一个整除 $a(a-Dc)(a+Dc)$ 而不整除 $2D$ 的素数. 如果 p 整除 a 和 c, 于是由问题 **2.a** 知 $v_p(a)=1$ 而 $v_p(c)\geqslant 2$, 从而有 $v_p(a-Dc)=1$ 和 $v_p(a+Dc)=1$ (问题 **1.b**), 故 $v_p(a(a-Dc)(a+Dc))=3$, 但由于 $a(a-Dc)(a+Dc)$ 是个平方数, 这是不可能的. 因此 p 不整除 (a,c), 从而只整除 $a,a-Dc,a+Dc$ 中的一个, 但由于这三个数的乘积是个平方数, 于是 $v_p(a),v_p(a-Dc),v_p(a+Dc)$ 中有两个是 0 而另一个是偶数.

3.a. 要证明有 $\varphi(P+Q)=\varphi(P)+\varphi(Q)$, 或者, 由于 $\varphi(P)=-\varphi(P)$, 证明 $\varphi(P+Q)+\varphi(P)+\varphi(Q)=0$. 如果 $P=\infty$ 或 $Q=\infty$, 则结论显然; 对于 $P+Q=0$ 的情形也是如此, 因为这时有 $x(P)=x(Q)$. 如果 $Q\notin\{P,-P\}$, 则公式 $\varphi(P+Q)+\varphi(P)+\varphi(Q)=0$ 由第 III 部分的问题 **2.b** 得到, 而如果 $Q=P$, 则由 III 的问题 **3.b** 有 $2\varphi(P)=0=\varphi(2P)$.

3.b. 如果 $Q=(x,y)\in C$ 满足 $2Q=P$, 那么 $x',x'-D,x'+D$ 在 $\mathbf{Q}$ 中为平方

数的假设条件告诉我们, 根据第 III 部分的问题 **3.b**, 存在有理数 a, b, c 使得有

$$\frac{x^2+D^2}{2y}=a, \quad \frac{x^2+2Dx-D^2}{2y}=b, \quad \frac{x^2-2Dx-D^2}{2y}=c.$$

因此有 $2a-b-c=\frac{2D^2}{y}$, 这证明了 y 是个有理数, 又有 $b-c=\frac{2Dx}{y}$, 这证明了 x 是个有理数, 故 $Q\in C(\mathbf{Q})$.

3.c. 如果 $P=(x,y)\in C(\mathbf{Q})$ 在 φ 的核中, 那么对任意的素数 p, $v_p(x)$ 和 $v_p(x+D)$ 都是偶数. 另一方面, 由于 $x\geqslant D$, 故有 $x>0$ 和 $x+D>0$ 以及由问题 **1.a** 知, x 和 $x+D$ 都是在 $\mathbf{Q}$ 中的平方数. 又由于 $x(x-D)(x+D)=y^2$ 为平方数, 由此得到 $x+D$ 也为平方数. 根据第 III 部分的 **6.d** 知, 方程 $2Q=P$ 至少在 C 中有一个解, 而前面的问题证明了 $Q\in C(\mathbf{Q})$, 而 $P\in 2\bar{C}(\mathbf{Q})$. 反之, 如果 $P=2Q, P\neq\infty, Q\in C(\mathbf{Q})$, 则第 III 部分的 **3.b** 证明了 x 和 $x+D$ 在 $\mathbf{Q}$ 中为平方数, 而 P 则在 φ 的核中. 因此, $\mathrm{Ker}\varphi=2\bar{C}(\mathbf{Q})$.

[637] **3.d.** 设 $Z\subset\bar{C}(\mathbf{Q})$ 是使得 φ 诱导了从 Z 到 $C(\mathbf{Q})$ 在 $(\mathbf{Z}/2\mathbf{Z})^{2s+2}$ 中的像上的一个双射. 于是 Z 有限 (因为它与一个有限集的子集有一个双射), 并且如果 $P\in\bar{C}(\mathbf{Q})$, 则存在 $R\in Z$ 使得 $\varphi(P-R)=0$; 因此存在 $Q\in\bar{C}(\mathbf{Q})$ 使得 $P-R=2Q$, 从而 $P=R+2Q$, 这便证明了 $\bar{C}(\mathbf{Q})$ 是 mod 2 有限型的.

IV.B

1. 如果 $2P=\infty$, 则无需证明什么. 否则, 如果 $2P=(x',y')$, 则根据第 III 部分的问题 **3.b** 有 $x'+D=(\frac{x^2+2Dx-D^2}{2y})^2$. 可将其重写为

$$x'+D=\frac{(\frac{a^2}{c^2}+2D\frac{a}{c}-D^2)^2}{4(\frac{a^3}{c^3}-D^2\frac{a}{c})}=\frac{(a^2+2Dac-D^2c^2)^2}{4ca(a-Dc)(a+Dc)}.$$

因此, 因为按照第 IV.A 部分的问题 **2.b** 知 c 和 $a(a-Dc)(a+Dc)$ 是平方数, 故 $c'=4ca(a-Dc)(a+Dc)$ 也是. 于是有

$$h(2P)\leqslant\log(c'(x'+D))=2\log((a+cD)^2-2D^2c^2)\leqslant 4\log(a+Dc)=4h(P).$$

2.a. 如果 d 整除 T, U 和 V, 则 d 也整除 $T+U+DV=2Da_1(a_2+Dc_2)$ 和 $T+U-DV=2Da_2(a_1+Dc_1)$. 因此它也整除 $(a_1+Dc_1)(T+U+DV)-2Da_1U=4D^3a_1c_1c_2$ 和 $(a_1+Dc_1)(T+U+DV)-2Da_1U-4D^3c_1V=4D^3a_2c_1^2$. 由对称性, 它也整除 $4D^3a_1c_2^2$.

2.b. 按照第 IV.A 部分的问题 **2.c** 知, $v_p(a_i)$ 是偶数, 又由第 IV.A 部分的问题 **2.a** 得到, 如果 $v_p(c_i)\neq 0$, 则 $v_p(a_i)\leqslant 1$; 它表明, 如果 $v_p(c_i)\neq 0$, 则 $v_p(a_i)=0$, 从而 p 不整除 a_i 和 c_i 的最大公因子.

现在, 由于 p 与 $4D^3$ 互素, 故 p 或整除 a_1 或整除 c_2. 若整除 a_1, 则它不整除 c_1, 从而整除 a_2, 因此它既不整除 c_2 也不整除 $a_1a_2+D^2c_1c_2$. 同样地, 如果它整除 c_2, 则它既不整除 a_2 也不整除 $a_1a_2+D^2c_1c_2$.

2.c. 设若相反; 有多种情形:

— p 整除 c_1 和 c_2; 那么按照第 IV.A 部分的问题 **2.a** 知, 在这种情形下 p^2 既不整除 a_1 也不整除 a_2, 并且 p^3 不整除 a_1a_2, 并由于 p^4 整除 c_1c_2, 故 p^3 也不整除 $a_1a_2 - D^2c_1c_2$; 故可排除这种情形.

— p 整除 c_1 但不整除 c_2, 这时 p^2 不整除 a_1, 且 p^5 不整除 $4D^3a_1c_2$; 这种情形因而也可排除, 对称地, 同样还有 p 整除 c_2 但不整除 c_1 的情形.

— p 既不整除 c_1 也不整除 c_2; 这时 p^2 整除 a_1 和 a_2, 但因为 D^2 不被 p^2 整除并且 a_1a_2 不被 p^4 整除, 故 $a_1a_2 + D^2c_1c_2$ 不被 p^5 整除; 这种情形也可以排除.

2.d. 只需将前面的问题 **3** 重新组合即可.

2.e. 设 c_3(分别地, c_4) 是使得 c_3x_3 (分别地, c_4x_4) 为整数的最小平方数. 令 $n = c_3c_4, a = \frac{d}{\delta}, b = \frac{d'}{\delta}, c = \frac{e}{\delta}$. 于是 a, b 和 c 之间互素, 并且 $\frac{na}{c} = \frac{nd}{e} = c_3x_3c_4x_4$ 以及 $\frac{nb}{c} = \frac{nd'}{e} = c_3(x_3+D)c_4(x_4+D)$ 都是整数. 于是存在整数 q, r, s 使得 $qa+rb+sc = 1$, 从而 $\frac{\delta c_3c_4}{e} = \frac{n}{c} = q\frac{na}{c} + r\frac{nb}{c} + sn$ 为整数. 现在由于一个 > 0 的整数是 $\geqslant 1$ 的, 故有

$$\begin{aligned}h(P_3) + h(P_4) &= \log(c_3(x_3 + D)) + \log(c_4(x_4 + D)) \\ &= \log(c_3c_4) + \log\frac{d'}{e} = \log d' - \log\delta + \log\frac{\delta c_3c_4}{e} \geqslant \log d' - \log\delta.\end{aligned}$$

2.f. 根据第 III 部分的问题 **5**, 我们有

$$x_3x_4 = \left(\frac{x_1x_2 - D^2}{x_1 - x_2}\right)^2 = \left(\frac{a_1a_2 - D^2c_1c_2}{a_1c_2 - a_2c_1}\right)^2,$$
$$(x_3 + D)(x_4 + D) = \left(\frac{a_1a_2 + D(a_1c_2 + a_2c_1) - D^2c_1c_2}{a_1c_2 - a_2c_1}\right)^2.$$

我们可以利用前一个问题, 其中 $d = (a_1a_2 - D^2c_1c_2)^2, d' = (a_1a_2 + D(a_1c_2 + a_2c_1) - D^2c_1c_2)^2$ 和 $e = (a_1c_2 - a_2c_1)^2$. 那么问题 **2.c** 证明了 d, d', e 的最大公因子 δ 整除 $(2D)^3$; 因此有 [638]

$$h(P_3) + h(P_4) \geqslant 2\log(a_1a_2 + D(a_1c_2 + a_2c_1) - D^2c_1c_2) - \log(2D)^3.$$

另外, 我们有

$$\begin{aligned}a_1a_2 + D(a_1c_2 + a_2c_1) - D^2c_1c_2 &= (a_1 + Dc_1)(a_2 + Dc_2) - 2D^2c_1c_2 \\ &= (a_1 + Dc_1)(a_2 + Dc_2)\left(1 - \frac{2D^2}{(x_1 + D)(x_2 + D)}\right),\end{aligned}$$

并由于 $x_1 \geqslant D, x_2 \geqslant D$, 故得到

$$a_1a_2 + D(a_1c_2 + a_2c_1) - D^2c_1c_2 \geqslant \frac{1}{2}(a_1 + Dc_1)(a_2 + Dc_2),$$

因此

$$h(P_3)+h(P_4)\geqslant 2\log\left(\frac{1}{2}(a_1+Dc_1)(a_2+Dc_2)\right)-\log(2D)^3$$
$$\geqslant 2(h(P_1)+h(P_2))-\log(32D^3).$$

3.a. 只需注意第 III 部分的问题 **2.a** 的公式即可.

3.b. 如果 $P=\infty$ 或 $P=(0,D)$, 则结果显然. 否则选取 $Q\notin\{P,-P,\infty,(0,D)\}$. 两次利用问题 **2.f**: 第一次让 $P_1=P+Q, P_2=P-Q$, 有

$$h(2P)+h(2Q)\geqslant 2(h(P+Q)+h(P-Q))-2\log(2(2D)^3)$$
$$\geqslant 4(h(P)+h(Q))-6\log(2(2D)^3),$$

从而利用问题 **1** 的不等式 $4h(Q)\geqslant h(2Q)$ 便得到结果.

3.c. 如果 $P=\infty$ 或 $Q=\infty$, 则可取 $A=0$. 如果 $P=Q$ 或 $P=-Q$, 则根据前一个问题, 可取 $A=6\log(2(2D)^3)$, 而如果 $P\neq\pm Q$ 且 $(P,Q)\in C(\mathbf{Q})$, 根据问题 **2.f** 可取 $A=\log(2(2D)^3)$. 最后, 对于所有的情形可取 $A=6\log(2(2D)^3)$ 即可.

3.d. 对于 $P+Q$ 和 $P-Q$ 应用前一个问题, 便得到一个囿于下的不等式 $h(2P)+h(2Q)\geqslant 2(h(P+Q)+h(P-Q))-A$, 并由问题 **1** 知 $h(2P)\leqslant 4h(P)$ 和 $h(2Q)\leqslant 4h(Q)$, 故得到 $h(P+Q)+h(P-Q)\leqslant 2h(P)+2h(Q)+\frac{A}{2}$. 因此最后得到, 对于任意的 $(P,Q)\in\bar{C}(\mathbf{Q})^2$ 有

$$|h(P+Q)+h(P-Q)-2h(P)-2h(Q)|\leqslant A.$$

3.e. 设 $B>0$. 如果 $h(P)\leqslant B$, 则或是有 $P=\infty$ 或是存在满足 $a+Dc\leqslant e^B$ 的整数 a,c, 使得 $P=(\frac{a}{c},y)$. 由于这些整数的偶对的集合有限, 并对于每个 x 的值最多只有两个可能的 y 的值, 故对于任意的 $B>0$, 满足 $h(P)\leqslant B$ 的 P 的集合有限.

3.f. 根据第 IV.A 部分的问题 **3.d**, 群 $\bar{C}(\mathbf{Q})$ 是 mod 2 有限型的, 并且具有容许高; 从而可以利用第 I 部分的问题 **3.e** 的结果得到结论.

术语索引

(索引页码为原著页码, 见本书边栏)

C

D

R

S

T

W

X

Y

Z

数学陈述索引

(索引页码为原著页码, 见本书边栏)

人名索引

(索引页码为原著页码，见本书边栏)

A

B

C

D

F

G

H

编　　年

(页码为原著页码, 见本书边栏)

1956, 谷山丰 – 韦伊猜想, 513, 522
1958, 格罗滕迪克革命发端, 133, 421
1958, $\mathbf{Z}_p$ 上的连续函数, 198, 477
1959, ζ 函数的有理性问题, 522
1960, BSD 猜想, 3
1960, 佐藤 – 泰特猜想, 421
1962, Bateman-Horn 猜想, 429
1964, p-adic ζ 函数, 487
1964, $\mathbf{Z}_p$ 上的局部解析函数, 484
1965, 连续函数的傅里叶级数几乎处处收敛, 290
1966, 所有集合是可测的, 300
1967, 朗兰兹纲领, 527
1969, 2 个变元的丢番图方程, 516
1970, 希尔伯特第 10 问题的否定解, 516
1971, ℓ^2 的一个特征刻画, 286
1973, 拉马努金 – 皮特森猜想的证明, 421
1973, $\mathbf{Z}_p$ 上的 $\mathscr{C}^k$ 函数, 479
1973, 对有限域上簇的黎曼假设, 421
1973, 大魔群存在性的预测, 232
1975, 几乎是孪生的素数有无限多, 429
1977, "moonshine" 的出现, 232
1977, 德利涅猜想, 2
1977, RSA 安全系统, 10
1977, 科兹 – 怀尔斯定理, 511
1978, 有无限多个 n 使 n^2+1 几乎是素数, 430
1979, $\zeta(3)$ 是无理数, 298, 520
1979, Waldspurger 定理, 514
1981, Enflo 的反例, 267
1982, 构造大魔群, 232
1982, p-adic 复数, 7, 197
1983, 同余数的确定, 506
1983, 莫德尔猜想的证明, 516, 520
1983, 格罗斯 – 察基尔定理, 511
1984, 塞尔猜想, 513
1984, p-adic 函数的零点, 488
1985, 伯林森猜想, 2
1985, abc 猜想, 53
1985, 梅尔滕斯猜想的否定, 444
1987, 基本引理, 552
1988, 基尔的 "ε-猜想" 的证明, 513
1989, 布洛赫 – 加藤猜想, 2
1989, 科里瓦金定理, 511
1992, "moonshine" 的释意, 232
1994, 费马大定理的证明, 232, 510, 522
1996, ℓ^2 的特征刻画, 284
1998, n^2+m^4 为素数的无限性, 430
1999, 谷山丰 – 韦伊猜想的证明, 510, 522
1999, 局部朗兰兹的对应, 551
1999, 对函数域的朗兰兹对应, 551
2000, 无限多个 $\zeta(2n+1)$ 为无理数, 298
2004, 素数构成的算术级数, 430
2005, 素数之间的微小差异, 429
2006, $r(E)$ 可能 $\geqslant 28$, 511
2006, 素数的多项式级数, 430
2008, 基尔猜想的证明, 529
2008, 基本引理的证明, 552
2008, $2^{43112609}-1$ 是素数, 427
2008, $Y^2-Y=X^5-X$ 的解, 517
2009, $\mathbf{B}_{\mathrm{cris}}^{\varphi=1}$ 是主理想环, 49
2009, 佐藤 – 泰特猜想的证明, 421
2010, 取素数的线性方程组, 430
2011, 平均地 $r(E)\leqslant 0,98$, 511

译后记

这是一本非常有特色的数学书. 从内容来说, 它是从教材发展出来的却不像一本教材, 因为它包含了许多非教材的文字 (譬如第 1 章的小词典以及 7 个附录), 它也不像某种数学专题读物, 既有代数也有分析还有许多数论专题. 这大概反映了作者所说的数学的统一性吧.

从背景来说, 也如作者所说, 它反映了法国高等教育体系的一个特殊方面. 在法国, 独立于普通大学体系存在一个精英体系, 包括了像成立于 1794 年的巴黎高等师范学院 (ENS) 和巴黎综合理工大学 (École Polytechnique), 等等. 要进入这些精英大学必须经过激烈的竞争, 先进入预科班然后再竞争方能入校. 作者曾长期执教于巴黎综合理工大学, 本书便是从他所教课程发展而来的, 所以包含了预科班的一些数学知识 (主要在第 1 章中), 我想这大体相当于我们大学一二年级和部分三年级的代数和分析的内容. 要是有人想考数学研究生的话, 这倒是代数和分析的很好参考材料. 第二部分的材料应该出现在我们的大学高年级和研究生一二年级相应的内容中了. 对于执着于数学研究的学生们, 我以为这是一本值得读的好书, 至少就本书而言应是如此, 特别地, 它还包含大量有分量的习题 (第 1 章有解答, 其他的部分习题和解答在附录 H1—7 中), 若能独立做出其中的大部分, 必将有大的进益.

由于作者是位资深的数论学家, 所以作为附录的第三部分主要讲述了所学内容在数论方面的应用, 证明或讲述了几个经典的大定理, 甚至有些内容还把我们带到了研究的第一线. 这当然对有志于数论的人大有裨益, 即便不想从事数论研究的人也不妨阅读譬如附录 A (看看素数定理是怎样证明的, 黎曼假设是怎样想的), 还有譬如附录 C (有限群的表示是如何计算的) ……浏览一下, 选出感兴趣的再仔细阅读, 从中发现学数学的乐趣和我们所学到的这些数学是多么强大和有用. 我所惋惜的是这本书几乎没有涉及几何学, 特别是代数几何. 它在数论中也是极其重要的.

作者还是一位极有个性的数学家. 最近, 因与校方观点不和而愤然辞职, 回到了法

国国家研究中心. 他对数学文化和数学教育抱有很大的热情和独到的见解, 它们洋溢在本书的字里行间, 特别是那些脚注颇值得一读. 由于法国的数学用语和习惯与我们有些不同, 我也做了一些脚注.

本书涉及的内容很多, 译者水平有限, 难免有所疏漏. 翻译中在内容和文字方面我请教了不少同事, 在此一并谢过. 同样, 感谢高等教育出版社的赵天夫先生在多方面的帮助.

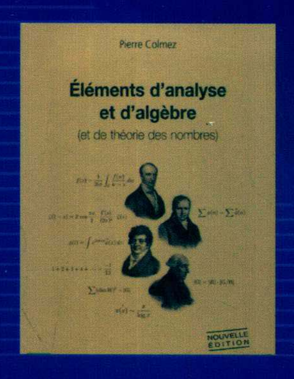
原书有 650 多页, 十分庞大, 并且字体极小 (作者曾调侃要读者带上放大镜), 读起来颇不方便. 为读者着想, 高等教育出版社做了有益的改变, 对此我和可能的读者们深表谢意.

译者

2017 年 12 月于北京

相关图书清单

序号	书号	书名	作者
1	9787040243086	解析函数论初步	H. 嘉当
2	9787040251562	微分学	H. 嘉当
3	9787040284171	广义函数论	L. 施瓦兹
4	9787040258011	微分几何——流形、曲线和曲面（修订第二版）	M. 贝尔热 等
5	9787040263626	拓扑学教程——拓扑空间和距离空间、数值函数、拓扑向量空间（第二版）	G. 肖盖
6	9787040251555	谱理论讲义（第二版）	J. 迪斯米埃
7	9787040246193	拟微分算子和 Nash–Moser 定理	S. 阿里纳克 等
8	9787040294675	解析与概率数论导引	G. 特伦鲍姆
9	9787040322941	概率与位势（第一卷）——可测空间	C. 德拉歇利 等
10	9787040319606	无穷小计算	J. 迪厄多内
11	9787040332384	分布系统的精确能控性、摄动和镇定（第一卷）——精确能控性	J.–L. 利翁斯
12	9787040287578	代数学教程	R. 戈德门特
13	9787040351767	完全集与三角级数	J.–P. 卡安
14	9787040477481	线性与非线性泛函分析及其应用（上册）	P. G. 希阿雷
15	9787040477498	线性与非线性泛函分析及其应用（下册）	P. G. 希阿雷
16	9787040495003	分析与代数原理（及数论）（第一卷）（第 2 版）	P. 科尔梅
17	9787040498691	分析与代数原理（及数论）（第二卷）（第 2 版）	P. 科尔梅





这本书源自巴黎综合理工大学的一年级课程，全书主要内容包括：

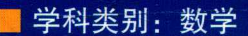
● “数学小词典”以更紧凑的形式给出了如下数学基本概念的要点：群、环、域、矩阵、拓扑、紧性、连通性、完备性、数值级数、函数序列的收敛性、埃尔米特空间等。同时包含一百多个习题及解答。

● 讲述数学根基中的 3 个理论：有限群表示论、经典泛函分析和全纯函数理论。

● 13 个“问题校正”综合了书中的定理用以证明一些漂亮的结果（如证明 $\zeta(3)$ 是无理数）。

本书的主要特色在于强调数学的文化特性和数学的统一性。许多脚注都暂时离开数学的“主干道”而进行一次别样的“短途观光”。7 个附录在课程内容范畴内讲述了经典数学文献的一些专题，展示如何结合这些基本理论来解决有深刻内涵的问题。其中之一是关于素数定理，它的证明经历了 150 多年才完成；另一个则是介绍了 Langlands 纲领，数论学家已经围绕它工作了 40 多年，其中一个最为精彩的结果是它蕴含了费马大定理。在这两者之间，读者会发现 p-adic 的一些特性，发现实数与 p-adic 数间带有神秘色彩的联系公式，或者看到未解决的千禧年问题。




学科类别：数学

academic.hep.com.cn


ISBN 978-7-04-049869-1
9 787040 498691 >
定价 99.00 元